CNS/ATM-1 Package SARPs and Guidance Material

Sub-Volume 5 - Internet Communications Service

Version 4.1

15 April 1996

Modifications inserted between V4.0 and V4.1 of CNS/ATM-1 Package Draft SARPs and Guidance Material, Sub-volume 5

Related chapter	Description of the modifications	Related CP or decision
Chapter 2 *Agreed DRs from WP221*	The editorial mistake in 2.4.3 has been corrected in conformance with CCB decision on 96030037.CP	96030037.CP, based on agreed DRs from WG2-WP/221 (Action 7/10 of Brisbane WG2/7)
Chapter 2 *Security Classification*	This CP has been agreed at the CCB meeting in Washington. Section 2.7.1 « The ATN Security Label » now includes 3 subsections: 2.7.1.1 Traffic Types 2.7.1.2 ATSC Class 2.7.1.3 Security Classification	96030040.CP, following Action 7/14 of Brisbane WG2/7
Chapter 2 *Support of SDU Size*	Change has been implemented in section 2.5.1.5 as specified in the CP (minimum SNSDU size of 1100 octets)	96040059.CP, as agreed at CCB meeting, Washington
Chapter 3 *Inconsistent description re: Supported RIB_Atts*	Note 1 of section 3.6 has been modified in accordance with the CCB decision on 96040052.CP	96040052.CP,as agreed at CCB meeting, Washington
Chapter 3 *Deficient Air/Ground Route Terminatin Procedure*	Section 3.5.2.12 Air/Ground Route Termination has been modified according to the CP.	96040054.CP, as agreed at CCB meeting, Washington
Chapter 3 *Action 7/12: ISH Hold Timer expiration*	Section 3.5.2.9 has been modified according to the CCB Decision on 96030039.CP.	96030039.CP, as agreed at CCB meeting, Washington
Chapter 3 *Action 7/11: initIDRP-xx APRLs items*	Section 3.5.2.13 APRLs have been modified according to 96030038.CP (true/false inversion for ListenForOpen in IDRP startup procedures)	96030038.CP, as agreed at CCB meeting, Washington
Chapter 3	The modifications proposed in 96030037.CP have been implemented	96030037.CP, as

Action 7/10: Agreed DRs from WP221	as agreed by CCB. These modifications impact: - section « 3.5.2.2.1.1. Call Request Failure », - section « 3.5.2.13 APRL for Air/Ground Route Initiation »	agreed at CCB meeting, Washington, based on discussions from WG2/7 concerning WG2-WP/221
Chapter 3 *ATSC Class*	Sections 3.7.1.2 c), 3.7.3.1 d) and 3.7.3.2. f) have been appended as specified in the CCB Decision field related to 96040056.CP	96040056.CP, as agreed at CCB meeting, Washington
Chapter 3 *Duplicated Specification*	Last paragraph of section 3.8 has been deleted because it was duplicating 8.3.1.6.3.d	96040065.CP, as agreed at CCB meeting, Washington.
Chapter 3 *Missing Rules for Creation of Routes to BISs*	Specification of the RD_HOP_COUNT value and Capacity value have been added to section 3.5.2.11.1.b, as agreed by CCB.	96040066.CP, as agreed at CCB meeting, Washington
Chapter 3 *Inconsistent Note on Routing Policy*	Modification has bene inserted in section 3.7.1.1 as specified in the CP	96040061.CP, as agreed at CCB meeting, Washington
Chapter 3 *Defect in NPDU Forwarding Rules*	The CP has been implemented in section 3.2.1.	96040067.CP, as agreed at CCB meeting, Washington
Chapter 4 *RD Selector in NSAP figure*	The modifications (replace routing domain identifier by routing domain) have been made to 4.5.6.1.1 and 4.5.6.1.2 Figure 4-1 has not yet been modified (replace Routing Domain Identifier by Routing Domain Selector) due to non availability of the designer tool	96030034.CP following Brisbane WG2/7 discussion on the meaning of « Routing Domain Identifier » (ISO meaning versus IDRP meaning)
Chapter 5 *Specification of TP4 Timer Values*	Section 5.4.1.1. « Transport Timer Values » has been added to the SARPs, concerning the recommended initial set of COTP Timer Values.	96030043.CP, with modifications inserted at CCB meeting, Washington
Chapter 5 *Incorrect Table Reference*	Reference to Table 2-2 has been changed to Table 2-3 where appropriate in Chapter 5. Furthermore, bullet 5 of section 5.2.2.1 has been revised to make the terms used in this bullet 5 and in Table 2-3 consistent.	96040049.CP, as agreed at CCB meeting, Washington
Chapter 5 *Misleading Title - Section 5.1.2*	Title of section 5.1.2 changes from « Internet Service description » to « Transport Service description »	96040053.CP, as agreed at CCB meeting, Washington
Chapter 6	As agreed in Brisbane, the CNS/ATM-1 Package Support for the XIDL APRL item has been changed from M to **XClra:O**	96030041.CP, as agreed in Brisbane

XIDL APRL Item		WG2/7 (discussion about WG2-WP/221)
Chapter 6 *Support of SDU Size*	Section 6.3.1.6 has been modified according to the CP. The APRL entry for NSS-s (section 6.4.2) has been changed to IS:M, ^IS:O	96040059.CP, as agreed at CCB meeting, Washington
Chapter 7 *Action 7/10: Agreed Drs from WP221*	Table 7-6 has been modified according to the CCB decision on 96030037.CP. Decimal diagnostic values for ATN call clearing have been added to the table.	96030037.CP, reflecting agreed Brisbane WG2/7 discussions about WG2-W¨/221
Chapter 7 *Action 7/4: refernece to router in CIDIN SNDCF*	The CP has been implemented based on agreed 95010031.DR In sections 7.7.2.4 and 7.7.2.5, « router » has been replaced by « **ATN system** »	96030036.CP, as agreed at CCB meeting, Washington
Chapter 7 *Action 7/5: Mob SNDCF Error Report codes*	Section « 7.5.4.8 SNDCF Error Report » has been modifed in conformance with the CP (based on agreed DR 95010044.DR): ... f) reason = [0000 0101] - **reserved**	96030035.CP, as agreed at CCB meeting, Washington
Chapter 7 *Precision in compression negociation*	Precision has been added to section 7.5.4.3.5 as specified in the CP	96030048.CP, as agreed at CCB meeting, Washington
Chapter 7: *SNDCF processing of SN-UNITDATA request*	Conforming to the CCB decision on that CP, the following paragraph has been added to 7.5.4.5 Action following an SN-UNITDATA Request : « **If there is no virtual circuit which satisfies the PDU priority and Security requirement, then the SNDCF shall try to establish a virtual circuit with adequate security and with the PDU priority**. »	96030047.CP, as agreed at CCB meeting, Washington
Chapter 7 *Support of SDU Size*	Last sentence of the first paragraph and following note of section 7.3.2 have been deleted conforming to the CP.	96040059.CP, as agreed at CCB meeting, Washington
Chapter 7 *Invalid Reference (7.10.1)*	Reference to section 7.5.4.1 in the APRL of section 7.10.1, items 'mcLocRef', 'mcACA' and 'mcV42' has been replaced by reference to section 7.5.4	96040064.CP, as agreed at CCB meeting, Washington
Chapter 8: *Inconsistent title: Table 8-5*	Table 8-5 has been renamed « 8-5: ISO 10747 Mandatory Requirements, for Which Support is Optional for ATN Airborne Routers »	96040055.CP, as agreed at CCB meeting, Washington.
Chapter 8 *Specified RIB_Att*	First paragraph of section 8.3.1.12 has been modified in accordance with the CCB Decision concerning 96040051.CP	96040051.CP, as agreed at CCB meeting, Washington.

Negotiation Requirements		
Chapter 8 *ATSC Class*	Encoding of the ATSC Class in the IDRP Security Parameter has been modified according to the decision made on 96040056.CP « Table 8-4 Identification of supported ATSC Class » has been created. Section 8.3.1.4.2 has been appended (c) created) as described in the CCB Decision field of 96040056.CP	96040056.CP, as agreed at CCB meeting, Washington
Chapter 8 *Route Aggregation and Information Reduction*	Section « 8.3.1.6 Route Aggregation and Route Information Reduction» has been modified in accordance with the agreed CP. « Table 8-5 ATN Routers and Route Aggregation » has been created	96040057.CP, as agreed at CCB meeting, Washington.
Chapter 8	As a consequence of the implementation of 96040056.CP and 96040057.CP, and of the creation of Table 8-4 and Table 8-5, Table 8-4 from version 4.0 becomes Table 8-6, and Table 8-5 becomes Table 8-7 The reference to those table has been checked in the overall SARPs.	consequence from 96040056.CP and 96040057.CP
Chapter 8 *Use of IDRP Security Tags*	Additional text has been appended to the end of section 8.3.1.2. New section « 8.3.1.13 Additional Update PDU Error Handling » has been inserted at the end of section 8.3.1.	96040058.CP, as agreed at CCB meeting, Washington
Chapter 8 *Specification of Classified Data*	Sections 8.3.1.5 and 8.3.1.4.3 have been modified according to the CCB decision on 96040060.CP	96040060.CP, as agreed at CCB meeting, Washington
Chapter 8 *Route Aggregation Rule*	« any » has been replaced by « at least one » in section 8.3.1.6.3.d, as specified in the CP.	96040063.CP, as agreed at CCB meeting, Washington
Chapter 8 *Permissible Traffic Type Requirement*	section 8.3.1.4.1 has been modified in accordance to the CP	96040062.CP, as agreed at CCB meeting, Washington.
Chapter 8 *Phase 2 IDRP Problem*	The CP has been implemented as specified in section 8.3.1.5	96040068.CP, as agreed at CCB meeting, Washington
Chapter 8 *Generation of ATSC Class Attribute*	The modifications of section 8.3.1.4.2, bullet a) have been inserted as specified in the CP.	96040069.CP
Chapter 8 *Security Parameter Settings in BISPDUs*	New section « 8.3.1.14 CLNP Data PDU Parameters » has been inserted at the end of 8.3.1.	96030044.CP, as agreed at CCB meeting, Washington

Editor's note:

Guidance Material is currently under development

Foreword

In January 1989, the Air Navigation Commission (ANC) expanded the terms of reference of the Secondary Surveillance Radar Improvements and Collision Avoidance Systems Panel (SICASP) to include the development of ICAO material as necessary to permit, to the maximum extent practicable, systems commonality and interoperability between ATS data links, including satellite data links.

The task emerged from the work of the Special Committee on Future Air Navigation Systems (FANS) which emphasized the need for the interchange of digital data over dissimilar aeronautical data links. The committee also recommended that the principles of the International Organization for Standardization (ISO) open systems interconnection (OSI) architecture be applied in developing aeronautical data links in order to provide for their interoperability.

Subsequent studies undertaken by the SICAS Panel resulted in the concept of the aeronautical telecommunication network (ATN) which is intended to support computer-to-computer communications operated by civil aviation authorities and aeronautical operating agencies. At its fourth meeting (March 1989), the SICAS Panel developed a description of the ATN and recommended it be published as an ICAO manual. The first edition of the manual was published in 1991, and the second edition was subsequently developed by the SICAS Panel and recommended for publication at the fifth meeting of the panel, (November 1993), and is expected to be published by ICAO during 1996. The development of the ATN continues with the objective of recommending Standards and Recommended Practices (SARPs) and Guidance Material for the ATN during 1996, for inclusion in Annex 10 at that time.

Following the completion of the work on the ATN Manual (Second Edition) by the SICAS Panel, the Air Navigation Commission transferred the work of developing SARPs and Guidance Material for the ATN to the ATN Panel (ATNP). At its first meeting, (ATNP/1, June 1994), it was agreed that the ATNP develop draft SARPs & guidance material for the "CNS/ATM-1 Package" which was to include the technical provisions for the internet, the upper layers and a limited set of initial air/ground and ground/ground applications in order to define the initial operational implementation of the ATN. This document, "Sub-Volume V" of the "CNS\ATM-1 Package", contains the draft SARPs and Guidance Material for the Internet (i.e. network & transport layers) component of the ATN, as derived from the material in the ATN Manual (second edition) by the ATN Panel Working Group 2 (WG2). Sub-Volume 1 contains introductory material to the CNS/ATM-1 Package, and additionally "system level" provisions applicable to the Package as a whole. Sub-Volume II contains provisions for the initial set of air/ground applications i.e. Automatic Dependent Surveillance (ADS), Controller Pilot Data Link Communications (CPDLC) , Flight Information Services (FIS) & Context Management (CM). Sub-Volume III contains provisions for the initial set of ground/ground applications i.e. Inter-Centre Communications (ICC) and Aeronautical Message Handling Service (AHMS). Sub-Volume IV contains provisions for the Upper Layer Architecture (ULA) to be supported by CNS/ATM-1 compliant End Systems.

This document will be maintained and updated by the ATNP WG2 during the development and validation of these draft SARPs and Guidance Material, resulting in validated material expected for recommendation to the ANC at ATNP/2 in November 1996. During this period, this document and its change history will be available to all interested parties.

Please note that the material in this document contains references to the documents of the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU). In using these documents, due attention should be given to their publication dates as shown on the list of references.

GLOSSARY

Abstract syntax. A notation which enables data types to be defined, and values of those types specified, without determining the way in which they will be represented (encoded) for transfer by protocols.

Accounting Management. Accounting management enables charges to be established for the use of resources, and for costs to be identified for the use of those resources. Accounting management includes functions to inform users of costs incurred or resources consumed, enable accounting limits to be set and tariff schedules to be associated with the use of resources, and enable costs to be combined where multiple resources are invoked to achieve a given communications objective.

A*ddress Domain*. An Address Domain is a set of address formats and values administered by a single address authority. Under the ISO plan, any address authority may define *subdomains* within its own domain, and delegate authority within those subdomains.

A*ddressing Authority*. An Addressing Authority defines formats and/or values of NSAP addresses within its jurisdiction.

Administrative Domain. A collection of end systems, intermediate systems and subnetworks operated by a single organization or administrative authority. An administrative domain may be internally divided into one or more routing domains.

Aeronautical Administrative Communications (AAC). Communications used by aeronautical operating agencies related to the business aspects of operating their flights and transport services. These communications are used for a variety of purposes, such as flight and ground transportation bookings, deployment of crew and aircraft or any other logistic purposes which maintains or enhances the efficiency of overall flight operation.

Aeronautical Administrative Messages. Messages regarding the operation or maintenance of facilities provided for the safety or regularity of aircraft operation, messages concerning the functioning of the aeronautical telecommunication services, and messages exchanged between government civil aviation authorities relating to aeronautical services.

Aeronautical Industry Service Communication (AINSC). AINSC comprises aeronautical industry communications between airlines, aeronautical industry service providers, general aviation operators, and any other industry stakeholders. This term is used for purposes of address administration.

AINSC Administrative Domain. An AINSC Administrative Domain is an ATN Administrative Domain owned and/or administered by an aeronautical industry service organization.

AINSC Routing Areas. An AINSC Routing Area is a routing subdomain comprising one or more ISs, and optionally, one or more ESs owned and/or administered by an aeronautical industry service organization. For example, an AINSC Routing Area may correspond to a physical location such as an airline's systems located at an airport.

AINSC Routing Domains. An AINSC Routing Domain comprises ESs and ISs that are part of an AINSC Administrative Domain.

AINSC RDC. The ATN AINSC RDC consists of all AINSC RDs in the ATN.

Aeronautical Information Service Messages. Messages concerning NOTAMS and messages concerning SNOWTAMS.

Aeronautical Mobile Satellite Service (AMSS). AMSS provides packet-mode data and circuit-mode data and voice service to aircraft and ground users provided by a satellite subnetwork that comprises satellites, Aircraft Earth Stations (AESs), Ground Earth Stations (GESs) and associated ground facilities such as a network coordination center.

Aeronautical Operational Control (AOC). Communications required for the exercise of authority over the initiation, continuation, diversion or termination of a flight in the interest of the safety of the aircraft and the regularity and efficiency of flight.

Aeronautical Passenger Communications (APC). Communications relating to the non-safety voice and data services to passengers and crew members for personal communications.

Aeronautical Telecommunication Network (ATN). The Aeronautical Telecommunication Network is an internetwork architecture that allows ground, air-to-ground and avionics data subnetworks to interoperate by adopting common interface services and protocols based on the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) reference model.

ATN host computer. An ATN host computer is a civil aeronautical computer system that contains one or more end user applications and which communicates using the ATN internet. In OSI terms, it denotes an End System. An ATN Host Computer may also implement the upper layers necessary to support the Systems Management Agent and Systems Management Manager and upper layer protocols as specified for the supported end-user applications.

ATN Internet (ATNI). An implementation of the ISO OSI network layer services and protocols for support of interprocess data communication between aeronautical host computers. It is defined to be the collection of the connected internetwork routers and subnetworks that conform to ATN internetwork requirements.

ATN Island Backbone RDC. An ATN backbone is an RDC comprising a subset of Transit Routing Domains within an ATN Island that provide general connectivity.

ATN Island Bridge. A bridge between two ATN Islands is a communications link between backbones over a suitable subnetwork.

ATN Island RDC. An ATN Island is an RDC comprising CAA-operated ATN RDs within a geographical region, and may include associated ATN service providers, or an RDC comprising Aeronautical Industry members which are users of communications services of a single Aeronautical Industry Service Provider, or more than one such provider providing services in combination with each other.

ATN Presentation Address. In the ATN, presentation addresses must, as a minimum, include an NSAP Address and a TSAP Selector and may include a PSAP Selector and SSAP Selector based on the addressing structure adopted within the ES and whether the application requires the OSI session or presentation protocol.

ATN Router. The communication element that manages the relaying and routing of data while in transit from an originating ATN host computer to a destination ATN host computer. In ISO terms, an ATN router comprises an OSI intermediate system and an end system supporting a systems management agent.

ATN Routing Domain Confederation. The ATN RDC is the set of interconnected RDs that together form the ATN.

Air Traffic Control(ATC). ATC is a service operated by an appropriate authority to promote the safe, orderly and expeditious flow of air traffic.

Air Traffic Services (ATS). Services provided by governmental civil aviation authorities.

Air Traffic Management (ATM). ATM consists of a ground and air part, both needed to ensure the safe and efficient movement of aircraft during all phases of operation.

Air Traffic Services Communications (ATSC). Communications related to air traffic services including air traffic control, aeronautical and meteorological information, position reporting and services related to safety and regularity of flight. This communication must involve one or more air traffic service administrations. This term is used for purposes of address administration.

ATSC Administrative Domain. An ATSC Administrative Domain is an ATN Administrative Domain owned and/or administered by an air traffic services organization.

ATSC RDC. The ATN ATSC RDC consists of all ATSC RDs in the ATN.

ATSC Routing Areas. An AINSC Routing Area is a routing subdomain comprising one or more ISs, and optionally, one or more ESs owned and/or administered by an ATS organization. For example, an ATSC Routing Area may correspond to a physical location such as an airport.

ATSC Routing Domain. An ATSC Routing Domain comprises ESs and ISs that are part of an ATSC Administrative Domain.

Application Entity (AE). Part of an application process which is concerned with communications within the OSI environment. The aspects of an application process which need to be taken into account for the purposes of OSI are represented by one or more AEs.

Application Layer. The layer of the OSI reference model that controls application user access to the communication system.

Application process (AP). A set of resources, including processing resources, within a real open system that may be used to perform a particular information processing activity.

Application Service Element (ASE). A set of functions that provide OSI communications capabilities for the interworking of AEs for a specific purpose. An AE may be composed of one ASE or several ASEs of different types.

Application Control Service Element (ACSE). The association control service element (ACSE) establishes, maintains and releases associations between application entities.

Automatic Dependent Surveillance (ADS). A technique for aircraft surveillance that is based upon the reporting of aircraft-derived position via a communication system.

Boundary Intermediate System (BIS). An intermediate system which is able to relay data between two separate routing or administrative domains.

Broadcast Subnetwork. Broadcast subnetworks (e.g. LANs) are often used to connect ISs and ESs within a small geographical area with media offering relatively high data throughput with relatively low delays.

Configuration Management. Configuration management identifies, exercises control over, collects data from and provides data to open systems for the purpose of preparing for, initializing, starting, providing for the continuous operation of, and terminating interconnection services.

Connectionless mode Service (CL). The communication service technique transfers data between peer layers without prior coordination. All protocol data units (PDUs) are transferred with no explicit association between them.

Connection mode Service (CO). The communication service technique which transfers data between peer layers using a prior connection to logically associate the sequence of protocol data units (PDUs).

Data Communications Equipment (DCE). An interface between data terminal equipment and the transmission mechanism.

Data Link Layer. The layer of the OSI reference model that manages the operations of the physical layer and may utilize special error detection or retransmission techniques to achieve acceptable error rates.

Data Terminal Equipment (DTE). A digital data transmitter/receiver device that includes terminals and computers.

Datagram service. A service providing the transmission and reception of packets of data as discrete messages.

Distinguishing Path Attribute (DPA). In ISO/IEC 10747 a DPA is used to discriminate among multiple routes to a destination, based on differences in the quality of service between the routes (for example, expense, transit delay or residual error probability.)

Domain. A set of end systems and intermediate systems which operate according to the same routing procedures and which is wholly contained within a single Administrative domain.

Domain Specific Part (DSP). An Addressing Authority is responsible for its own Addressing Subdomain, and NSAP Addresses within that addressing domain are distinguished, where necessary, by the value of the DSP.

End Routing Domain (ERD). A RD that only routes PDUs from/to its own RD.

End System (ES). A system that contains the seven OSI layers and contains one or more end user application processes.

Entity. An active element in any layer which can either be a software entity (such as a process) or a hardware entity (such as an intelligent I/O chip).

Ethernet. Ethernet is based on a local area network standard ISO 8802-3 *Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications* using broadcast technology which may connect as an ATN subnetwork.

Expected Quality of Service (QOS). Expected QOS is based on a combination of a priori knowledge and analysis of performance information received from the operation of routing protocols.

Expected Transit Delay. Expected Transit Delay is defined as the time elapsed between the invocation of CLNS by the source ATN NS user and the arrival of an NSDU at the destination ATN NS user, based on an NPDU size of 512 octets. Transit Delay values are expressed in increments of 500 milliseconds.

Expense. Expense is the cost to perform some task. In the context of internetworking, expense is defined in terms of the incremental expense incurred for transfer of a single NSDU of 512 octets in size.

Fault Management. Fault management encompasses fault detection, isolation and the correction of abnormal operation, and includes functions to maintain and examine error logs, accept and act upon error detection notifications, trace and identify faults, carry out sequences of diagnostic tests and correct faults.

Fixed ATN RDC. The Fixed ATN RDC consists of all ground-based RDs that form the ATN.

Flow control. A function which controls the flow of data to perform buffer management within a layer or between adjacent layers.

Forwarding Information Base (FIB). The information base that is maintained by each ATN router and contains the set of forwarding paths reflecting the various policy and QOS rankings available to reach each known destination.

Gateway. A system used to interconnect dissimilar networks. A gateway may contain all seven layers of the OSI reference model.

General Communications. A category of communications that includes APC, public correspondence, and other non-operational and non-administrative communications.

General Topology Subnetwork. General topology subnetworks (e.g. WANs) are often used to connect geographically dispersed ISs and ESs.

Global Network Addressing. An internetwork addressing plan covering world-wide aeronautical operations which enables all participating subnetworks to function in a single integrated global network.

Global Network Addressing Domain. An addressing domain consisting of all the NSAP addresses in the OSI environment.

Indicated QOS. Indicated QOS is determined by the QOS parameters passed in protocol control information, and may reflect varying accuracy with respect to actual characteristics.

Initial Domain Part (IDP). The IDP identifies the Addressing Authority responsible for an Addressing Subdomain which assigned the NSAP Address, and which specified the abstract syntax and structure of the remainder of the NSAP Address.

Integrated Services Digital Network (ISDN). A public telecommunications network that supports the transmission of digitized voice and data traffic on the same transmission links.

Intermediate System (IS). A system comprising the lower three layers of the OSI reference model and performing relaying and routing functions.

Internetwork. A set of interconnected, logically independent heterogeneous subnetworks. The constituent subnetworks are usually administrated separately and may employ different transmission media.

Internetwork Protocol. A protocol which performs the basic end-to-end mechanism for the transfer of data packets between network entities. In the ATN Internet, the ISO 8473 internetwork protocol is used.

Interoperable. Describes the ability of the ATN to provide, as a minimum, a transparent data transfer service between end systems even though the ATN comprises various ground, air-to-ground, and avionics subnetworks. The ability to interoperate between end systems can be extended to include commonality of upper layer protocols.

Intra-domain routing information exchange protocol. In the ATN, the ISO 10589 IS-IS intra-domain routing information exchange protocol may be used to exchange connectivity and topology information between ATN routers within a routing domain.

Level 1 subdomain. A routing subdomain of end systems and intermediate systems which maintains detailed routing information about its own internal composition and routing information which allows it to reach other routing areas. A level 1 subdomain area is also denoted a routing area.

Level 2 subdomain. The subset of all level 2 intermediate systems within a routing domain.

Local Area Network (LAN). A network connecting various data communication devices in a localized geographical area such as a single aircraft, office building or a group of buildings.

Lower layers. A term pertaining to the physical, data link, network and transport layers of the OSI reference model.

Manager. A manager is the term given to a system which requests or otherwise receives information about managed objects.

Managed Object. Managed objects refer to those data processing and data communication resources that may be managed through the use of the OSI Management protocol.

Management Administrative Domain. A management administrative domain is a management domain where the managed objects in the domain are all under the responsibility of one and only one administrative authority.

Management Agent. The Management Agent performs management operations on managed objects within its local environment as a consequence of management operations communicated from a manager. An Agent may also forward notifications emitted by managed objects to a manager.

Management Domain. Management domains are resources which for systems management purposes are represented by managed objects. A management domain possesses at least the following quantities: a name which uniquely identifies that management domain, identification of a collection of managed objects which are members of the domain, and identification of any inter-domain relationships between this domain and other domains.

Mean Transit Delay. The average time it takes to transfer a standard packet size from source to destination.

Message. Information which is passed in one or more data blocks from one end user to another through different subnetworks.

Multi-homed End Routing Domain. An ERD that is in communication with more than one RD.

Management Information Base (MIB). The management information base is a conceptual composite of management information within an open system.

Management Information System (MIS)-User. An MIS-User is a management application. For the purposes of network management, an MIS-User is allowed to take on one of two possible roles - either an agent role or a manager role.

Mobile Routing Domains. A mobile routing domain is formed from ATSC and AINSC systems on board an aircraft (or any other mobile platform), within the aircraft operator's Administrative Domain. A mobile RD is characterized as an End Routing Domain (ERD).

Mobile Subnetwork. A mobile subnetwork is a subnetwork connecting a mobile system with another system not resident in the same mobile platform. These subnetworks tend to use free-radiating media (e.g. VHF/UHF radio, D-band satellite or D-band secondary surveillance radar) rather than "contained" media (e.g. wire or coaxial cable); thus they exhibit broadcast capabilities in the truest sense.

Mode Select (Mode S). An enhanced mode of secondary surveillance radar (SSR) that permits the selective interrogation of Mode S transponders, the two-way exchange of digital data between Mode S interrogators and transponders, and also the interrogation of Mode A or Mode C transponders.

Network Addressing Domain. A subset of the global addressing domain consisting of all the NSAP addresses allocated by one or more addressing authorities.

Network Entity. A functional portion of an internetwork router or host computer that is responsible for the operation of internetwork data transfer, routing information exchange, and network layer management protocols.

Network Entity Title (NET). The global address of a network entity.

Network Layer. The ISO network layer is responsible for providing a uniform service interface for the transfer of data among end systems and intermediate systems (ISs) utilizing the ISO protocol architecture.

Network Service Access Point (NSAP). Point within the ISO protocol architecture at which global end users may be uniquely addressed on an end-to-end basis.

Network Service Access Point (NSAP) Address. The NSAP Address is a hierarchically organized global address, supporting international, geographical and telephony-oriented formats by way of an address format identifer located within the protocol header. Although the top level of the NSAP address hierarchy is internationally administered by ISO, subordinate address domains are administered by appropriate local organizations.

NSAP address prefix. NSAP Address prefixes are used to identify groups of systems that reside in a given routing domain or confederation. An NSAP prefix may have a length that is either smaller than, or the same size as, the base NSAP address.

Network Management. Network Management is the set of functions related to the management of various OSI resources and their status across the Network Layer of the OSI architecture.

Network Topology Map. Network topology maps provide an overall view of the global network connectivity, and are used in path computations by the operative routing algorithm.

Open Systems Interconnection (OSI) Protocol Architecture. A set of protocols used to implement the OSI reference model.

Open Systems Interconnection (OSI) reference model. A model providing a standard approach to network design introducing modularity by dividing the complex set of functions into seven more manageable, self-contained, functional layers. By convention these are usually depicted as a vertical stack.

Packet. The basic unit of data transfer among communications devices within the network layer.

Performance Management. Performance management enables the behavior of resources and the effectiveness of communication activities to be evaluated. Performance management includes functions to gather statistical information, maintain and examine logs of system state histories, determine system performance under natural and artificial conditions, and alter system modes of operation for the purpose of conducting performance management activities.

Physical Layer. The layer of the OSI reference model that controls access to the transmission medium that forms the basis for the communication system.

Policy Information Base (PIB). The PIB is contained with a BIS, and consists of a set of policy statements specified by the Systems Manager which together describe the applicable Routing Policy.

Presentation Layer. The layer of the OSI reference model that controls the coding, format and appearance of the data transferred to and from the application layer.

Presentation Service Selector (PSAP Selector). The element of the presentation address which identifies the user of the presentation protocol entity.

Priority. Priority is defined as the relative importance of a particular PDU relative to other PDUs in transit, and is used to allocate resources which become scarce during the transfer process.

Profile. A profile defines implementation conformance constraints on a set of reference specifications.

Protocol. A set of rules and formats (semantic and syntactic) which determines the communication behavior between peer entities in the performance of functions at that layer.

Protocol Control Information (PCI). Information included in a layer header which contains service primitives specific to that layer.

Protocol Data Unit(PDU). A unit of data transferred between peer entities within a protocol layer consisting of protocol control information and higher layer user data (i.e. service data units).

Quality of Service (QOS). Information relating to data transfer characteristics (for example, requested throughput and priority) used by a router to perform relaying and routing operations across the subnetworks which make up a network.

Relaying. The process of transferring packets across subnetworks including any necessary packet conversion.

Requested QOS. Requested QOS reflects the service characteristics desired by the service user.

Reserved Value. Reserved values constitute legal values for the respective fields but have not yet been assigned specific meanings by ICAO. These values should be processed normally in order to allow future assignment. Meanings may be assigned in the future and are not available for local use. The allocation of these values requires no change in the version identifier.

Residual Error Probability. Residual Error Probability indicates the likelihood that an PDU will be lost, duplicated or corrupted. This probability is defined as the ratio of lost, duplicated or corrupted NSDUs to the total number of NSDUs transmitted by an ATN NS provider, normalized for an NSDU size of 512 octets.

Route. A route consists of the set of addresses which identifies the destinations reachable over the router, and information about the route's path including the QOS and security available over the route.

Router. A router is the communication element that manages the relaying and routing of data while in transit from an originating end system to a destination end system. An ATN router comprises an OSI intermediate system and end system supporting a systems management agent.

Routing. A function within a layer which uses the address to which an entity is attached in order to define a path by which that entity can be reached.

Routing Area(RA). A routing area is a routing subdomain comprising one or more ISs, and optionally one or more ESs.

*Routing Domain.*A set of end systems and intermediate systems which operate the same routing protocols and procedures and which are wholly contained within a single administrative domain. A routing domain may be divided into multiple routing subdomains.

Routing Domain Confederation (RDC). A Routing Domain Confederation (RDC) is a set of Routing Domains and/or RDCs which have agreed to join together and form a Routing Domain Confederation. The formation of a RDC is done by private arrangement between its members without any need for global coordination.

Routing Domain Identifier (RDI). An RDI is a generic NET as described in ISO 7498, and is assigned statically in accordance with ISO 8348. An RDI is not an address, and cannot be used as a valid destination of an ISO 8473 PDU. However, RDIs are, like ordinary NETs, assigned from the same Addressing Domain as NSAP Addresses.

Routing Information Base(RIB). A data base which is maintained by each router and comprises the information regarding the connectivity and topology of the ESs and ISs within a particular Routing Domain and path information pertinent to paths interconnecting Routing Domains. It is maintained by way of the information received by a routing information exchange protocol. Each Routing Information Exchange Protocol has its own RIB specification.

Routing information exchange protocol. The protocol used to exchange subnetwork connectivity information between end systems and intermediate systems and between intermediate systems and intermediate systems.

Routing Policy. The set of rules in a BIS which determines the advertisement and use of routes is known as a Routing Policy. Each organizational user of the ATN must determine and apply their own Routing Policy.

Safety Case. A safety case is an analysis presenting an overall justification for the declaration that a particular systems satisfies its safety requirements.

Security Label. A Security Label may indicate requirements for protection of a PDU and provide information used by network layer access control functions.

Security Management. The purpose of security management is to support the application of security policies by means of functions which include the creation, deletion and control of security services and mechanisms, the distribution of security-relevant information and the reporting of security-related events.

Service Data Unit. A unit of data transferred between adjacent layer entities, which is encapsulated within a PDU for transfer to a peer layer.

Session layer. The layer of the OSI reference model that establishes the rules of dialogue between two end-user entities.

Session Service Selector (SSAP Selector). The element of the session address which identifies the user of the session protocol entity.

Single Homed ERD. An ERD that is in communication with one other RD only.

Spare Value. A Spare value is a value for which no meaning is currently defined. These values are available by the administering authority for local use, and may be assigned in the future.

Stack (or protocol stack). A set of cooperating OSI protocols selected from different layers of the basic reference model. Hence, "upper layer stack" refers to session, presentation and application protocols, while "lower layer stack" refers to physical, data link, network and transport protocols.

Subnetwork. An actual implementation of a data network which employs a homogeneous protocol and addressing plan, and is under control of a single authority.

Subnetwork Access Facility (SNAcF). The subset of the OSI network layer which provides the interface with the data link layer and is specific to a particular subnetwork.

Subnetwork Access Protocol (SNAcP). The actual protocol used to receive services form a particular subnetwork. For example, the subnetwork access protocol to many public data networks is X.25.

Subnetwork Dependent Convergence Function (SNDCF). The set of rules and procedures needed to convert the data transfer needs of the subnetwork independent convergence protocol to the actual services provided by a subnetwork.

Subnetwork Domain. The set of end systems and intermediate systems connected to the same physical network.

Subnetwork Independent Convergence Function (SNICF). The subnetwork independent convergence protocol is the common protocol for all ATN host computers and routers that is used for the transfer of data. In the ATN internet, the SNICF is the connectionless network protocol defined by ISO 8473.

Subnetwork Point of Attachment (SNPA). The SNPA is the point at which a real end system, interworking unit, or real subnetwork is attached to a real subnetwork, and is a conceptual point within an end or intermediate system at which the subnetwork service is offered.

*Subnetwork Point of Attachment (SNPA) Address.*The SNPA address provides information used in the context of a particular real subnetwork to identify a SNPA. An SNPA address is a subnetwork address such as X.25 DTE Addresses, Ethernet MAC Addresses, etc.

Subnetwork sublayer. A component of the OSI reference model that provides the protocol mechanism for data transfer between peer entities within the same subnetwork. This sublayer is an implementation of the OSI subnetwork access facility (SNAcF).

Systems Management. Systems Management is the set of functions related to the management of various OSI resources and their status across all layers of the OSI architecture.

Systems Management Application Entity (SMAE). The SMAE is an application entity for the purpose of systems management communications.

Systems Management Function. Systems Management Functions encompass the monitoring, controlling, operating, supervising, coordination and administration of a communications network.

Transit Routing Domain (TRD). A Transit Routing Domain is a domain whose policies permit its BISs to provide relaying for PDUS whose source is located in either the local routing domain or in a different routing domain.

Transport layer. The layer of the OSI reference model that assures reliable end-to-end transfer between transport service users.

Transport Service Access Point (TSAP). The Transport Service Access Point is the logical access point to the transport layer.

Transport Service Access Point (TSAP) address. The complete communications address which unambiguously defines a transport service user. The TSAP address comprises the NSAP address and a TSAP-selector.

*Transport Service Access Point Selector (TSAP Selector).*The element of the transport address which identifies the user of the transport protocol entity.

Transport service (TS) user. The entity which uses transport layer services.

Upper layers. A term pertaining to the session, presentation and application layers of the OSI reference model.

Very High Frequency (VHF). VHF is a frequency band from 30 to 300 megahertz.

*VHF Data Link (VDL).*VDL provides packet data communications to aircraft and ground users provided by a VDL subnetwork that comprises airborne VHF data radios (VDRs), VHF ground stations and connectivity to routers on the aircraft and the ground.

Virtual circuit priority. The priority associated with a connection (virtual circuit) which is established between two systems prior to the transmission of data.

Wide Area Network (WAN). Wide Area Networks are used to interconnect geographically dispersed routers and host computers. These subnetworks may be internally complex packet switching entities of their own, or they may be as simple as point-to-point dedicated lines.

X.25 Packet Switched Data Network (PSDN). An X.25 PSDN is a communications network that provides a network access service in compliance with CCITT Recommendation X.25.

ACRONYMS AND ABBREVIATIONS

AAC	Aeronautical Administrative Communications
ACA	Address compression algorithm
ACSE	Association control service element
AD	Administrative domain
AD	Addendum
ADJBISMO	Adjacent BIS MO
ADJRIBMO	Adjacent RIB MO
ADM	Administrative identifier
ADMF	ADM Flag
AE	Application entity
AES	Aircraft earth station
AFS	Aeronautical fixed service
AFI	Authority and format identifier
AINSC	Aeronautical Industry Service Communication
AK	Data acknowledgement
AMSS	Aeronautical mobile satellite service
ANC	Air Navigation Commission
AOC	Aeronautical Operational Communications
AOM	Systems Management Upper Layer profile
AP	Application process
APC	Aeronautical Passenger Communications
APRL	ATN profile requirements list
ARPA	Advanced Research Projects Agency
ARPANET	ARPA network
ARS	Administrative region selector
ARSD	ARS Default [Flag]
ASE	Application service element
ASN.1	Abstract Syntax Notation One
ATC	Air traffic control
ATFM	Air traffic flow management
ATM	Air traffic management
ATN	Aeronautical telecommunication network
ATNI	ATN internet
ATNPA	ATN protocol architecture
ATNSM	ATN systems management
ATS	Air traffic services

ATSC	Air Traffic Services Communications
BCD	Binary Coded Decimal
BER	Basic encoding rules
BIS	Boundary intermediate system
BISPDU	BIS PDU
BPS	Bits per second
BSI	British Standards Institute
C	Conditional
C	Counter
CAA	Civil aviation administration
CAN	Cancellation
CC	Connection confirm
CCITT	International Telegraph and Telephone Consultative Committee
CDT	Credit
CE	Congestion experienced flag
CIDIN	Common ICAO data interchange network
CL	Connectionless mode
CLNP	CL network protocol
CLNPMMO	CL network protocol machine MO
CLNS	CL network service
CLTP	CL transport protocol
CLTPMMO	CL transport protocol machine MO
CLTS	CL transport service
CMIP	Common management information protocol
CMIS	Common management information service
CMISE	CMIS element
CNS	Communications, navigation, and surveillance
CO	Connection mode
COMSEC	Communications security
COTP	CO transport protocol
COTPMMO	COTP protocol machine MO
COTS	CO transport service
CR	Connection request
CVER	Compressed VER
DC	Disconnect confirm
DCC	Data country code
DCE	Data circuit terminating equipment
DFDAU	Digital flight data acquisition unit
DOD	Department of Defense

DPA	Distinguishing path attribute
DR	Disconnect request
DSP	Domain specific part
DST-REF	Destination reference
DT	Data
DTE	Data terminal equipment
E/C	Error probability over cost flag
E/R	Error report requested
E/T	Error probability over transit delay flag
EA	ED acknowledge
ED	Expedited data
EGP	Exterior gateway protocol
EOT	End of TSDU
ER	Error [TPDU]
ER	Error report [NPDU]
ER	Error report requested flag
ERD	End routing domain
ERP	Echo Response [NPDU]
ERQ	Echo Request [NPDU]
ES	End System
ESCT	ES configuration timer
ESH	ES hello
EXP	LOCREF extension flag
F/M	Fixed/Mobile
FANS	Future Air Navigation Systems
FIB	Forwarding information base
FIBMO	FIB MO
FIFO	First in first out
FMS	Flight management system
FP	Full/Prefix
FSM	Finite state machine
FTAM	File transfer, access and management
G	Gauge
GA	General Aviation
GDMO	Guideline for definition of MOs
GES	Ground earth station
I	Out of scope
IATA	International Air Transport Association
IA-5	International Alphabet No. 5

ICAO	International Civil Aviation Organization
ICD	International code designator
ICS	Implementation conformance statement
ID	Identifier
IDI	Initial domain identifier
IDP	Initial domain part
IDRP	Interdomain routing protocol
IDRPCFGMO	IDRP configuration MO
IEC	International electrotechnical commission
IIH	IS-IS hello
IMF	International Monetary Fund
IOC	Internet operations center
IP	Internetwork protocol
IPI	Initial protocol identifier
IPRL	ISP Protocol RL
IS	Intermediate system
ISDN	Integrated Services Digital Network
IS-SME	IS SME
ISH	IS hello
ISN	Initial sequence number
ISO	International Organization for Standardization
ISOPA	ISO protocol architecture
ISORM	ISO reference model
ISP	International standardized profile
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector [c0 2985]
IUT	Implementation under test
IVMO	Initial value MO
k	Kilo
L1R	Level 1 Router
L2R	Level 2 Router
LAN	Local area network
LI	Length indicator
LINKMO	Linkage MO
LOC	Location identifier
LOCD	LOC Default [Flag]
LOCREF	Local reference
LOCRIBMO	Local RIB MO
LSP	Link state PDU

M	Mandatory
M	More [bit] (X.25)
MAC	Medium Access Control
MAD	Management administrative domain
MD	Management Domain
MET	Meteorological
MIB	Management information base
MIDS	Management information definition statement
MIS	Management information service
MO	Managed object
MOA	MO attribute
MOCS	MO conformance statement
MOD	Modulus
Mode S	Mode Select
MORTS	MO requirement template specification
MS	More segments flag
N/A	Not applicable
NATO	North Atlantic Treaty Organization
NE	Network entity
NEMO	NE MO
NET	NE title
NL	Network layer
NLE	NL entity
NLM	NL management
NLPI	NL protocol information
NLRI	NL reachability information
NLSP	NL security protocol
NM	Network management
NOTAM	Notice to airmen
NPAI	Network protocol address information
NPDU	Network protocol data unit
NS	Network service
NSMO	Network subsystem MO
NSAP	NS access point
NSAPMO	NSAP MO
NSDU	NS data unit
O	Optional
OCA	Object class attributes
OCN	Object class notifications

OCNB	Object class name bindings
OOC	Operations on object classes
OR	Operational requirements
OSI	Open systems interconnection
OSIE	OSI environment
OSIM	OSI management
OSISME	OSI SM environment
P	Priority
PC	Personal Computer
PCI	Protocol control information
PDAM	Proposed Draft Addendum
PDN	Public data network
PDU	Protocol data unit
PER	Packed encoding rules
PIB	Policy information base
PIBMO	PIB MO
PICS	Protocol implementation conformance statement
PSAP	Presentation service access point
PSDN	Packet switched data network
PTT	Post, telephone, and telegraph
Q	QOS Maintenance
QOS	Quality of service
R	Recommended
R	Read-only
R&R	Requirements and Recommendations
RA	Routing area
RD	Routing domain
RD PDU	Redirect PDU
RDC	Routing domain confederation
RDF	Routing domain format
RDFD	RDF Domain [Flag]
RDI	Routing domain identifier
RER	Residual error rate
RF	Radio frequency
RIB	Routing information base
RJ	Reject
RL	Requirements list
ROA	Request of Acknowledgement
ROSE	Remote operation service element

RP	Routing information exchange protocol
RPOA	Recognized private operating agency
RPF	Reference publication format
RTE	Receiving TE
RTSE	Reliable transfer service element
R/W	Read/write
S	W (creation), R (lifetime)
S/T	Segmentation over transit delay flag
SARPs	Standards and Recommended Practices
SDU	Service data unit
SEL	Selector
SICASP	SSR Improvements and Collision Avoidance Systems Panel
SM	Systems management
SMA	SM application
SMAE	SM AE
SME	SM entity
SMF	SM function
SMFA	SM functional area
SN	Subnetwork
SN-SME	SN SME
SNAcF	SN access function
SNAcP	SN access protocol
SNCR	SN connection reference
SNDCF	SN dependent convergence function
SNDCP	SN dependent convergence protocol
SNICF	SN independent convergence function
SNICP	SN independent convergence protocol
SNL	SN layer
SNOWTAM	Snow NOTAM
SNP	Sequence number PDU
SNPA	SN point of attachment
SNQOS	SN QOS
SNS	SN service
SNSDU	SN SDU
SP	SN Processor
SP	Segmentation permitted flag
SPI	Subsequent protocol identifier
SRC-REF	Source reference
SSR	Secondary surveillance radar

STE	Sending TE
SYS	System identifier
SYS4	SYS 4th Octet [Flag]
SYS5	SYS 5th Octet [Flag]
SYS6	SYS 6th Octet [Flag]
T	Tidemark
T/C	Transit delay over cost flag
TC	Transport connection
TCMO	TC MO
TCP	Transmission control protocol
TCIVMO	TC IVMO
TCQIVMO	TC QOS IVMO
TE	Transport entity
TEMO	TE MO
TLE	Transport layer entity
TP4	Transport protocol class 4
TPDU	Transport protocol data unit
TPDU-NR	TPDU send sequence number
TR	Technical report
TRD	Transit routing domain
TS	Transport service
TSAP	TS access point
TSAPMO	TSAP MO
TSDU	TS data unit
TSMO	Transport subsystem MO
TSN	Tag set name
U	User option
UD	Unit data
UHF	Ultra high frequency
VC	Virtual circuit
VDL	VHF data link
VER	Version
VHF	Very high frequency
WAN	Wide area network
WR	Receive window value
WS	Send window value
WX	Weather
X	Excluded
X	Hexadecimal

YR-TU-NR	expected TPDU sequence number (’your TPDU number’)
YR-EDTU-NR	expected ED TPDU sequence number in EA (’your ED TPDU number’)
-	N/A
^	Not

LIST OF REFERENCES

ISO 3166:1993	Codes for the representation of names of countries
ISO 6523:1984	Data interchange – Structures for the identification of organizations
ISO/IEC 7498-1:1994	Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model
ISO 7498-2:1989	Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture
ISO 7498-3:1989	Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 3: Naming and addressing
ISO/IEC 7498-4:1989	Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management framework
ISO/IEC 8072:1994	Information technology – Open Systems Interconnection – Transport service definition (*Note: re-issue that includes addendum 1)*
ISO/IEC 8073:1992	Information technology – Telecommunications and information exchange between systems – Open Systems Interconnection – Protocol for providing the connection-mode transport service
ISO/IEC 8208:1995	Information technology – Data communications – X.25 Packet Layer Protocol for Data Terminal Equipment
ISO/IEC 8348:1993	Information technology – Open Systems Interconnection – Network Service Definition (*Note: re-issue that includes addenda 1 and 2)*
ISO/IEC 8473-1:1994	Information technology – Protocol for providing the connectionless-mode network service: Protocol specification
ISO/IEC DIS 8473-2	Information technology – Protocol for providing the connectionless-mode network service – Part 2: Provision of the underlying service by an ISO/IEC 8802 subnetwork
ISO/IEC 8473-3:1995	Information technology – Protocol for providing the connectionless-mode network service: Provision of the underlying service by an X.25 subnetwork
ISO/IEC 8602:1995	Information technology – Protocol for providing the OSI connectionless-mode transport service (*Note: re-issue that includes amendment 1)*
ISO 8648:1988	Information processing systems – Open Systems Interconnection – Internal organization of the Network Layer
ISO/IEC 8802-2:1994	Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 2: Logical link control
ISO/IEC 8824:1990	Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1) *(Provisionally retained edition)*

ISO/IEC 8825:1990	Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1) *(Provisionally retained edition)*
ISO 9542:1988	Information processing systems – Telecommunications and information exchange between systems – End system to Intermediate system routeing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473)
ISO/IEC DIS 9542	Information technology – End system to Intermediate system routeing information exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO/IEC 8473) *(includes amendments 1 and 2)*
ISO/IEC TR 9575:1995	Information technology – Telecommunications and information exchange between systems – OSI Routeing Framework
ISO/IEC TR 9577:1993	Information technology – Telecommunications and information exchange between systems – Protocol identification in the network layer
ISO/IEC 10589:1992	Information technology – Telecommunications and information exchange between systems – Intermediate system to intermediate system intra-domain-routeing routine information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473)
ISO/IEC 10747:1994	Information technology – Telecommunications and information exchange between systems – Protocol for exchange of inter-domain routeing information among intermediate systems to support forwarding of ISO 8473 PDUs
ISO/IEC TR 10730:1993	Information technology – Open Systems Interconnection – Tutorial on naming and addressing
ISO/IEC 10731:1994	Information technology – Open Systems Interconnection – Basic Reference Model – Conventions for the definition of OSI services *(Note: replaces ISO TR 8509:1987 withdrawn in 1994)*
ISO/IEC 11577:1995	Information technology – Open Systems Interconnection – Network layer security protocol

1. INTRODUCTION

Note 1-

1.1 The SARPs for the CNS/ATM-1 Package are documented in five "Sub-Volume" as follows:

- *Sub-Volume I - Introduction & System Level Requirements*
- *Sub-Volume II - Air/Ground Applications*
- *Sub-Volume III - Ground/Ground Applications*
- *Sub-Volume IV - Upper Layer Architecture*
- *Sub-Volume V - Internet Communications Service*

1.2 This document comprises Sub-Volume V.

1.3 Sub-Volume V defines the provisions that Aeronautical Telecommunication Network compliant End Systems (ESs) and Intermediate Systems (ISs) must implement in order to provide a CNS/ATM-1 Package compliant "Internet Communications Service" to the "User" i.e. the Upper Layer Architecture as defined in Sub-Volume IV of the CNS/ATM-1 Package SARPs.

1.4 Sub-Volume V comprises nine Chapters as introduced below.

1.4.1 Chapter 1, i.e. this Chapter, contains introductory material to the remainder of the Sub-Volume.

1.4.2 Chapter 2 contains pertinent Internet definitions, system level provisions related to communications protocol support for ATN End Systems and Intermediate Systems, and SARPs related to priority handling within the ATN internet.

14.3 Chapter 3 contains provisions related to the definition of the ATN Internet Routing Architecture and components thereof e.g. Routing Domains, Administrative Domains, Routing Domain Confederations, ATN Backbone, ATN Islands, Routing Policies etc.

1.4.4 Chapter 4 contains provisions related to the ATN Internet addressing architecture and responsibilities related to the definition and allocation of ATN Internet address fields.

1.4.5 Chapter 5 contains "Transport Layer" provisions applicable to ATN End Systems. Provisions for the ISO Connection Oriented Transport Protocol (Class 4) and the Connectionless Transport Protocol are defined. The majority of such provisions are defined in a tabular fashion under the title of "ATN Protocol Requirements Lists" (APRLs) as are the provisions for the protocols defined in subsequent chapters of this Sub-Volume.

1.4.6 Chapter 6 contains "Inter-Network Layer" provisions ,based on the ISO Connectionless Network Protocol (CLNP), applicable to ATN End Systems and ATN Intermediate Systems.

1.4.7 Chapter 7 contains provisions related to the various candidate ground/ground and air/ground subnetworks of the ATN in order to ensure sucessful inter-operation of ATN Intermediate Systems and the subnetworks to which they are attached and to enable the efficient use of the limited bandwidth available over the currently standardised air/ground subnetworks via the definition of appropriate compression techniques.

1.4.8 Chapter 8 contains provisions related to the exchange of routing information between ATN Intermediate Systems and End Systems based on ISO OSI Routing Information Exchange protocols such as the Inter Domain Routing Information Exchange Protocol (IDRP).

1.4.9 Chapter 9 contains assumptions regarding the implementation of internet Systems Management within the frame of the CNS/ATM-1 Package.

2. DEFINITIONS AND CONCEPTS

2.1 Objectives and Goals

Note 1.— In computer data networking terminology, the infrastructure required to support the interconnection of automated ATM systems is referred to as an internet. Simply stated, an internet comprises the interconnection of computers with gateways or routers via real subnetworks. This allows the construction of a homogeneous virtual data network in an environment of administrative and technical diversity. Given the desire to interconnect an evolving and ever wider variety of aircraft- and ground-based computers to accomplish this ATM automation, it is clear that the civil aviation community needs a global data internet. The internetworking infrastructure developed by ICAO for this purpose is the ATN.

Note 2.— The ATN design allows communication services for different user groups, i.e. air traffic services (ATS), aeronautical operational control (AOC), aeronautical administrative communications (AAC) and aeronautical passenger communications (APC). The design provides for the incorporation of different air-ground subnetworks (e.g. SSR Mode S, AMSS, VDL) and different ground-ground subnetworks, resulting in a common data transfer service. These two aspects are the basis for interoperability of the ATN and will provide a reliable data transfer service for all users. Furthermore, the design is such that user communications services can be introduced in an evolutionary manner.

Note 3.— The ATN is capable of operating in a multinational environment with different data communication service providers. The ATN is capable of supporting ATSC as well as AINSC.

Note 4.— The ATN is capable of supporting the interconnection of End Systems (ES) and Intermediate Systems (IS) using a variety of subnetwork types.

2.2 Definitions

Note.— This specification makes extensive use of the definitions, concepts and terminology derived from the OSI Reference Model (ISO 7498 parts 1-4) and the OSI Routing Framework (ISO TR 9575).

2.2.1 The ATN Internet

The ATN shall consist of a set of interconnected Routing Domains (RDs), within the global OSI Environment (OSIE). Each such RD shall contain *Air Traffic Service Communication* (ATSC) and/or *Aeronautical Industry Service Communication* (AINSC) related Intermediate and End Systems. A Routing Domain that declares itself to be a Transit Routing Domain (TRD) shall implement a Routing Policy that supports the relaying of NPDUs received from at least one other Routing Domain to destinations in another Routing Domain. Otherwise, the Routing Domain shall be defined as an End Routing Domain (ERD).

2.2.2 ATN RDs

An ATN RD shall meet the requirements specified in ISO TR 9575 for a Routing Domain and shall include one or more ATN Routers.

Every ATN RD shall have a unique Routing Domain Identifier (RDI).

Note.— An RDI is a generic Network Entity Title (NET), and has the same syntax as an ATN NSAP Address; alias RDIs are permitted.

2.2.2.1 Administration RDs

Each Administration participating in the ATN shall operate one or more ATN RDs, comprising Air/Ground and Ground-Ground Routers as required to interconnect with Mobile RDs and other ground based ATN RDs, respectively.

Note.— Adjacent Administrations may alternatively combine their RDs into a single RD.

2.2.2.2 Aeronautical Industry RDs

Each aeronautical industry member participating in the ATN shall operate one or more Routing Domains (RDs), comprising Air/Ground and Ground-Ground Routers as required to interconnect with Mobile RDs and other ground based ATN RDs, respectively.

Note.— Adjacent aeronautical industry domains may alternatively combine their RDs into a single RD.

2.2.2.3 Mobile RDs

Each ATN equipped mobile platform (e.g. an aircraft), shall operate at least one ATN RD. This shall be an End Routing Domain. This ERD shall include ATSC and AINSC related Intermediate and End Systems contained within this mobile platform, and at least one Airborne Router (Router Class 6 or 7).

Note 1.— An ATN mobile platform may operate multiple ERDs.

Note 2.— When more than one Airborne Router is installed on board an aircraft, then each must be in a separate Routing Domain.

Recommendation.— *ATSC and AINSC End-Systems and Intermediate Systems located within a mobile platform should form a single Routing Domain, within the appropriate Administrative Domain.*

Note 3.— A single routing domain minimizes the transfer of routing information over low-bandwidth air-ground subnetworks.

Note 4.— It is anticipated that other classes of mobile platforms (e.g. airport surface vehicles, etc.) may be operated as ATN routing domains in the future.

2.2.3 The Ground ATN Internet

The Ground ATN Internet shall consist of one or more ATN Islands.

2.2.3.1 ATN Island

Each ATN Island shall comprise one or more ATN RDs forming a single ATN Island RDC.

An ATN Island shall not contain any ATN mobile RD.

Note. — An example ATN Island topology is presented in Figure 2-1

2.2.3.2 The Fixed ATN RDC

The Fixed ATN RDC shall comprise all ATN RDs other than Mobile RDs.

Note.— The Fixed ATN RDC enables a ground ATN Router to advertise a route to a mobile, the destination of which is the entire fixed ATN, without having to enumerate the RDIs of all ATN RDs in the RD_Path Attribute.

2.2.4 The Global ATN Backbone

The Global ATN Backbone shall comprise at least one ATN RD from each ATN Island, interconnected either directly or indirectly via other members of the Global ATN Backbone.

Note.— The purpose of the Global ATN Backbone is to provide a high availability core network of ATN Routers supporting ATN Mobile Routing.

2.2.4.1 ATN Island Backbone RDCs

Recommendation.— *Within each ATN Island, those ATN RDs that are members of the Global ATN Backbone should form a single RDC, the ATN Backbone RDC.*

An ATN Backbone RDC, when present, shall be nested within an ATN Island RDC.

Note 1 .— The purpose of the Backbone RDC is to permit more than one ATN RD to act as the default route provider for an ATN Island. It also provides a containment boundary to limit the impact of changes in routes to mobile RDs, to only the members of the Backbone RDC and not to the rest of the ATN Island.

Note 2.— This is only a recommended practice as in some regions, simpler, or other alternative structures may be more appropriate for an ATN Island.

2.2.5 The “Home” Domain

Aircraft for which inter-Island communications are required shall have a “Home” domain, which is a Routing Domain in an ATN Island.

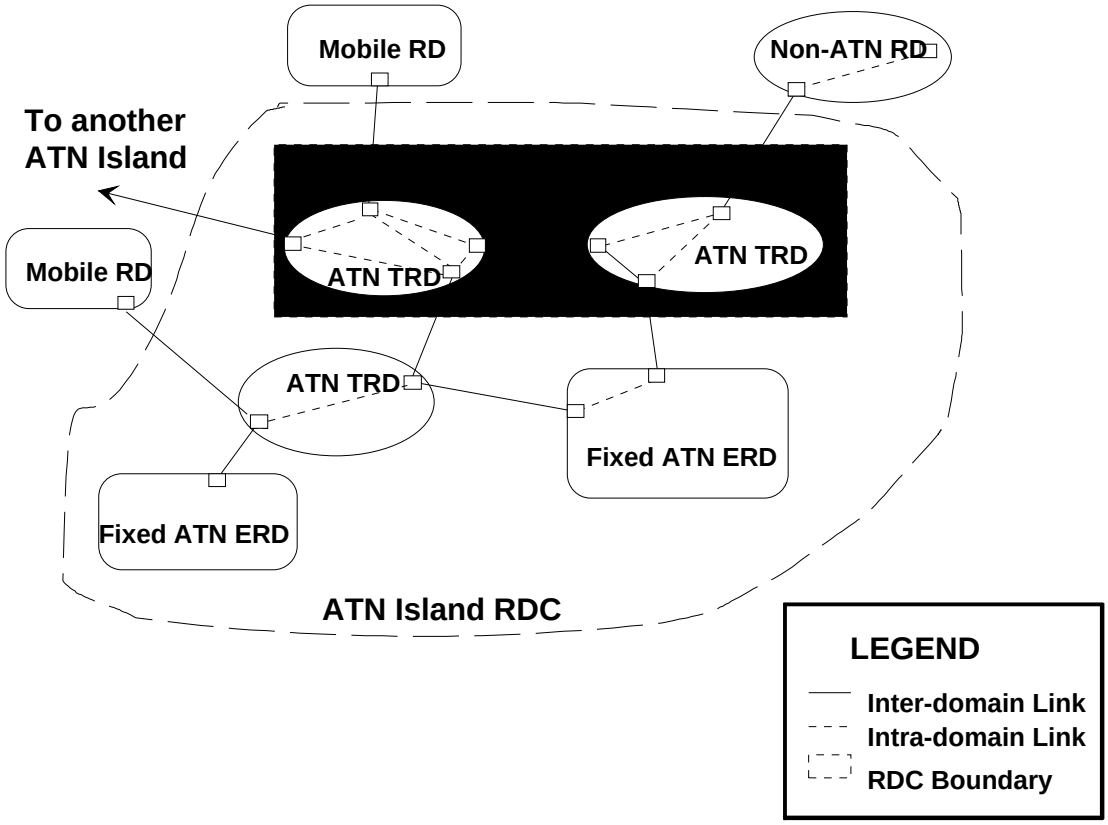


Figure 2-1 Example ATN Island Routing Domain Confederation Structure

Note 1.— This "home" needs not be in either the ATN Island through which the aircraft is currently reachable, or in the ATN Island with which communication is required.

Note 2.— The role of the "Home" domain is to advertise a default route to all the aircraft belonging to an airline, or the General Aviation aircraft of a given country of registration. This default route is advertised to the ATN Global Backbone in line with the routing policies specified in 3.7.

2.2.6 Administrative Domains and the ATN

The Administrative Domain of each administration, and aeronautical industry member that operates one or more ATN RDs shall comprise both their ATN RDs, and any non-ATN RDs that they operate.

Note.— The Routing Policies for communication between ATN and non-ATN RDs within the same Administrative Domain is a local matter.

2.3 ATN End Systems

Note 1.— ATN End Systems are capable of communicating with other ATN End Systems, either directly or indirectly, to provide end-to-end communication service for both air/ground and ground/ground applications.

Note 2. — An ATN End System is a realisation of the OSI End System architectural entity.

Note 3. — An ATN End System supports one or more ATN Applications and supports their communication over the ATN by providing either the connection mode transport service, or the connectionless mode transport service, or both.

2.3.1 Physical and Data Link Layer

ATN End Systems shall implement the appropriate Physical and Data Link Layer functions for access to the ATN subnetwork to which they are attached.

2.3.2 Network Layer

ATN End Systems shall implement:

a) The End System provisions of ISO 8473 - *Protocol for Providing the Connectionless Mode Network Service* - as the Subnetwork Independent Convergence Function (SNICF) as specified in Chapter 6.

b) a Subnetwork Access Protocol (SNAcP) suitable for each underlying subnetwork.

c) a Subnetwork Dependent Convergence Facility (SNDCF) providing byte and code independent service to the SNICF (i.e ISO 8473) via the selected Subnetwork Access Protocol, as specified in Chapter 7.

Recommendation.— *ATN End systems should implement:*

d) The End System provisions of ISO 9542 - End-System to Intermediate System Routing Exchange Protocol for use in conjunction with the Protocol for the Provision of the Connectionless-mode Network Service- to facilitate the exchange of routing information between the ES and any locally attached IS(s).

2.3.3 Transport Layer

Depending on the requirements of the application and its supporting upper-layer protocols, ATN End Systems shall implement either one or both of the following:

a) ISO 8073 - *Connection-Oriented Transport Protocol (Class 4)* - as specified in Chapter 5.

b) ISO 8602 - *Connectionless Transport Protocol* - as specified in chapter 5.

2.3.4 Upper Layers

Note 1.— The requirements for session, presentation and application layer protocols to support end-user applications on ATN End-Systems are defined in Sub-volume 4 of the CNS/ATM-1 SARPs.

2.3.5 Applications

Note 1. — The requirements for CNS/ATM-1 air/ground and ground/ground applications are contained in Sub-volumles 2 and 3 of the CNS/ATM-1 SARPs respectively.

2.4 ATN Routers

Note 1.— ATN Routers are capable of the relaying and routing of Network Layer protocol data units with other ATN Routers and with directly connected ATN End Systems.

Note 2. — An ATN Router is a realisation of the OSI Intermediate System architectural entity. ATN Routers that additionally implement ISO 10747 are also known as Boundary Intermediate Systems (BISs).

2.4.1 ATN Router Classes

The classes of ATN Router and the Routing Protocols supported, that are recognised by this specification, are listed below in Table 2-1:

Class	Name	Routing Protocols Supported
1.	Static Router	ISO 9542 (optional)
2.	Level 1 Router	ISO 9542 (optional) ISO/IEC 10589 Level 1 only
3.	Level 2 Router	ISO 9542 (optional) ISO/IEC 10589 Level 1 and Level 2
4.	Ground-Ground Router	ISO 9542 (optional) ISO/IEC 10589 (optional) ISO/IEC 10747
5.	Air/Ground-Router (ground based)	ISO 9542 ISO/IEC 10589 (optional) ISO/IEC 10747 Route Initiation Procedures (see 3.5.2)

Class	Name	Routing Protocols Supported
6.	Airborne Router with IDRP	ISO 9542 ISO/IEC 10747 Route Initiation Procedures (see 3.5.2)
7.	Airborne Router without IDRP	ISO 9542 Route Initiation Procedures (see 3.5.2)

Table 2-1 ATN Router Classes

Note 1.— Classes 1, 2 and 3 are only for use within an ATN Routing Domain and their specification is a local matter.

Note 2.— The intra-domain parts of Router Classes 4 and 5 are also a local matter.

Note 3. — The intra-domain part of Router Class 6 and 7 are concerned with the interconnection of avionics to the airborne router and are the subject of aeronautical industry standards.

Note 4.— Router Classes 5, 6 and 7 describe routers that support at least one ATN Mobile Subnetwork.

All ATN Inter-Domain Routers (i.e. Router Classes 4 to 7 inclusive) shall support:

a) the ISO 8473 Connectionless Network Protocol (CLNP) as specified in Chapter6, including the use of the CLNP options security parameter, and shall interpret and obey the Routing Policy Requirements expressed therein, whilst routing the packet in accordance with any restrictions placed on the traffic types that may be carried over a given ATN Subnetwork, by forwarding CLNP NPDUs according to 3.8.

b) the ISO 10747 Inter-Domain Routing Protocol (IDRP) as specified in Chapter8 for the exchange of inter-domain routing information according to 3.6 and 3.7.

An Airborne (Router Classes 6 or 7) or Air/Ground Router (Router Class 5) shall support the Mobile SNDCF specified in Chapter7 for the use of CLNP over an ATN Mobile Subnetwork, and the ISO 9542 ES-IS routing information exchange protocol, as specified in Chapter8 for support of the route initiation procedures specified in 3.5.2.

2.4.2 Physical and Data Link Layers

ATN Routers shall implement the appropriate Physical and Data Link Layer functions for access to the ATN subnetwork(s) to which they are attached..

2.4.3 Network Layer

An ATN Router shall implement:

a) the Intermediate System provisions of ISO 8473 - *Protocol for Providing the Connectionless Mode Network Service* - as the Subnetwork Independent Convergence Function (SNICF) as specified in Chapter6.

b) a Subnetwork Access Protocol (SNAcP)suitable for each underlying subnetwork.

c) a Subnetwork Dependent Convergence Facility (SNDCF)providing byte and code independent service to the SNICF (i.e. ISO 8473) via the selected Subnetwork Access Protocol., as specified in Chapter7.

d) The routing protocols specified in Table 2-1 for the Router's Router Class, as specified in Chapter8.

e) The Route Initiation procedures appropriate to the Router Class, as specified in chapter3.

f) Where an ATN Router is directly connected to one or more mobile subnetworks, it shall implement a sub-set of the ISO 9542 - End-System to Intermediate System Routing Exchange Protocol for use in conjunction with the Protocol for the Provision of the Connectionless-mode Network Service - for operation over those subnetworks to facilitate the exchange of addressing (BIS Network Entity Title) information between the Router and its peer as specified in Chapter3 (see 3.5.2) and in Chapter 8.

ATN Routers of class 5 (Air/Ground Routers) and of class 7 (Airborne Routers without IDRP) shall also implement the mechanisms necessary to support the "optional non-use of ISO 10747" ~~where the~~ as specified in Chapter3;

Recommendation.— *All ATN Airborne Routers should support the use of ISO 10747. (i.e. Class 6 is the perferred Airborne Router Class).*

Note.— Some States may require that aircraft operating in their airspace, after July 1999, and desiring ATSC services via the ATN must support the use of ISO 10747, as specified in Chapter8.

2.5 ATN Subnetworks

Note .— An ATN Subnetwork is any fixed or mobile data communications network that fulfils the following requirements.

2.5.1 Requirements for All ATN Subnetworks

Both fixed and mobile ATN subnetworks shall conform to the following requirements :

2.5.1.1 Byte and Code Independence

Data shall be transferred through ATN Subnetworks in a byte and code independent manner.

Note. — If necessary, this byte and code independence may be ensured through the services of the SNDCF.

2.5.1.2 Subnetwork QOS

Subnetwork QOS shall either be constant and known, or must be capable of being determined on a dynamic basis, in order to support the internetwork routing decision process.

Note. — The service referred to is the quality of the SN-Service, which may differ from the inherent subnetwork QOS where an SNDCF is employed.

2.5.1.3 Subnetwork Addressing

An ATN subnetwork shall provide a mechanism for uniquely and unambiguously identifying each ATN router attached to that subnetwork.

2.5.1.4 Internal subnetwork routing

Routing between specified SNPA addresses on a local subnetwork shall be carried out by mechanisms internal to the subnetwork, based solely on the subnetwork addressing information given to the SN-Service provider when the SN-Service is invoked.

2.5.1.5 Minimum SNSDU Size

An ATN subnetwork shall support a minimum ~~n~~ SNSDU size ~~of a minimum~~ of 1100~~068~~ octets.

Note 1. — The 1100 octet number is derived from a 1024 octets user data, 9 octets fixed ISO 8473 header, 42 octets Source and Destination NSAP Addresses, 4 octets for the SNDCF local reference option, 3 octets for the QoS Maintenance parameter, 3 octets for the priority parameter, and 15 octets for the security parameter.

Note 2. — This will permit the use of the non-segmenting ISO 8473 subset for NSDUs of up to 1024 octets.

2.5.2 Requirements for Mobile ATN Subnetworks

An ATN mobile subnetwork shall conform to the following requirements

2.5.2.1 Invocation of Subnetwork Priority

When priority is implemented within that subnetwork, an ATN subnetwork shall provide a SNAcP mechanism for invocation of subnetwork priority.

2.5.2.2 Invocation of Subnetwork Quality of Service for Mobile Subnetworks

Recommendation.— *Mobile ATN Subnetworks should provide a mechanism for invocation of subnetwork QOS. Subnetwork QOS parameters include transit delay, protection against unauthorized access, cost determination and residual error probability.*

Note.— ATN subnetworks may allocate subnetwork resources on a per user or per subnetwork connection basis in order to make available a different QOS.

2.5.2.3 Connection-Mode Subnetwork Service

An ATN mobile subnetwork shall provide a connection-mode service between SNPAs, with a well-defined start and end to a connection, and with reliable, sequenced SNSDU transfer over that connection. When QOS is available on a per subnetwork connection basis, the SNAcP shall provide mechanisms for selecting a specific QOS when the subnetwork connection is established.

Note 1.— A mobile subnetwork implementing ISO 8208 to provide a connection-mode service between SNPAs meets this requirement; however, where appropriate, an alternative protocol providing the same service may be used.

Note 2.— This requirement does not imply the need for a single mobile SNAcP.

2.5.2.4 Connectivity Status Changes

Note 1. — Mobile ATN subnetworks may provide a mechanism for detection of change in media connectivity and for the conveyance of this information to connected ATN routers.

If a mobile subnetwork provides subnetwork connectivity information, the subnetwork shall convey this information to connected subnetwork service users (i.e. connected ATN routers), in order to initiate operation of the internetwork routing protocols as specified in Chapter3.

Note 2. — It is desirable for the IS-SME to be notified as soon as possible by the SN-SME when communication is possible with a newly attached BIS and for an immediate decision to be made as regards bringing up the link.

2.5.2.5 Segmentation/Reassembly Mechanism

Recommendation.— *An ATN subnetwork should provide a mechanism that allows the conveyance of large SNSDUs greater than the subnetwork's internal packet size between subnetwork points of attachment.*

Note.— It is the responsibility of the subnetwork to ensure that this data is efficiently segmented and/or concatenated for efficient transfer over the physical medium. If this capability is not present within a Mobile ATN Subnetwork, ISO 8473 can support segmentation of NPDUs for transit over subnetworks with small maximum SNSDU sizes.

2.6 Quality of Service Concept

Note 1. — In the ATN, the Quality of Service provided to applications is maintained using Capacity Planning techniques that are outside of the scope of this specification. Network Administrators are responsible for designing and implementing a network that will meet the QoS requirements of the CNS/ATM applications that use it.

Note 2. —Network Administrators may take advantage of the strong QoS requirements signalled by the ATC Class (see Security Concept), in order to ensure that only those parts of the ATN that support the high QoS requirements of ATSC applications, need be designed to meet those requirements.

2.7 ATN Security Concept

Note 1. —ATN Security Functions are concerned with:

a) Protecting CNS/ATM applications from internal and external threats;

b) Ensuring that application Quality of Service and Routing Policy Requirements are maintained, including service availability; and,

c) Ensuring that air-ground subnetworks are used in accordance with ITU requirements.

Note 2. —Other than through the provision of physical security mechanisms, no security mechanisms are provided in the ATN Internet for protecting CNS/ATM applications. CNS/ATM Applications need to develop their own security mechanisms for countering any threats to their proper operation.

Note 3. —There are currently no mechanisms for protecting the Routing Information Base from an attacker. However, the use of ISO 10747 type 2 authentication is under consideration for specification in future versions of this specification.

Note 4. —The ATN Internet does provide mechanisms to support items (b) and (c) above. These mechanisms are defined to take place in a common domain of trust, and use a Security Label in the header of each CLNP Data PDU to convey information identifying the "traffic type" of the data and the application's routing policy and/or strong QoS Requirements. No mechanisms are provided to protect the integrity of this label or its binding to the application data.

Note 5. — In order to permit the later extension of the ATN to handle classified data, the Security Label in the CLNP Data PDU header can additionally be used to convey Security Classification information.

Note 65. — The Routing Information necessary to support this security label is maintained through

information conveyed in the ISO 10747 Security Path Attribute about each route. ATN Routers of classes 4 and above reference this routing information during the NPDU forwarding process in order to meet the application's requirements expressed through the NPDU's security label and to enforce any applicable ITU restrictions.

2.7.1 The ATN Security Label

The ATN Security Label shall be encoded according to section 6.2.2.1.

An ATN Security Label shall be provided as part of the header of every CLNP NPDU, except for those that convey General Communications Applications data.

Note 1. — The above implies that any CLNP NPDU that does not contain an ATN Security Label contains General Communications data.

2.7.1.1 Traffic Types

An NPDU's Security Label shall identify the "Traffic Type" of its user data, as either:

a) ATN Operational Communications - ATSC

b) ATN Operational Communications - AOC

c) ATN Administrative Communications

d) ATN Systems Management.

For the ATN Operational - ATSC traffic type, routing policy requirements shall be expressed through further information encoded into the Security Label, as:

a) An ATSC Class, or

b) An ordered preference for the class of air-ground subnetwork used to convey the data; the only order that may be expressed is Mode S, VDL, AMSS and finally HF, or

c) No routing policy preference.

For the ATN Operational - AOC traffic type, routing policy requirements shall be expressed through further information encoded into the Security Label, as either no routing policy preference, or an ordered list of appropriate air-ground subnetworks to be used.

Note 2. —The possible ordering are specified in table 6-1.

2.7.1.2 ATSC Class

ATSC Class shall be used to convey the strong Quality of Service requirements, if any, of ATSC Applications. The ATSC Class shall be expressed as a class identifier in the range A to H.

The Transit Delay semantics of ATSC Class are defined in Table 2-2.

ATSC Class	Maximum (95%) end-to-end Transit Delay (Seconds)
A	Reserved
B	Reserved
C	13
D	18
E	Reserved
F	74
G	95
H	Reserved

Table 2-2 ATSC Transit Delay Semantics

Note. — The semantics of the ATSC Classes for other QoS metrics and availability, are outside of the scope of this specification.

2.7.1.3 Security Classification

The Security Classification may be used to convey the confidentiality level of Applications data.

2.7.2 Applications use of ATN Security Labels

ATSC and AISC applications shall specify an ATN Security Label for each message category that they support. This ATN Security Label shall identify:

a) the Traffic Type appropriate for the message; and,

b) for ATN Operational applications, the application's requirements for the routing of the message, if any, expressed as specified in 2.7.1.

When sent using the connection mode transport service, a message shall only be conveyed over a transport connection which is associated with the same ATN Security Label as that specified for the message's message category.

When sent using the connectionless transport service, the TSDU conveying that message shall be associated with the ATN Security Label specified for the message's message category.

2.7.3 Transport Layer Security

2.7.3.1 In the Connection Mode

Except when a transport connection is used to convey general communications data, each transport connection shall be associated with a single ATN Security Label. The value of this label shall be determined when the connection is initiated.

Note 1. —It is not possible to change an ATN Security Label during the lifetime of a transport connection.

Every NSDU passed to the Network Layer that contains a TPDU from a transport connection associated with an ATN Security Label shall be associated with the same ATN Security Label.

Note 2. — The network layer functions may then encode this ATN Security Label in the NPDU header.

TPDUs from transport connections associated with different ATN Security Labels shall not be concatenated into the same NSDU.

When an incoming CR TPDU is received, the ATN Security Label, if any, encoded into the NPDU header of the NPDU that conveyed it, defines the ATN Security Label that is associated with the transport connection.

Note 3. —The mechanism by which the connection initiator determines the appropriate ATN Security Label is a local matter. For example, it may be identified by an extension to the transport service interface, be implicit in the choice of a given TSAP, or be identified using a Systems Management function.

Note 4. — Some applications may reject incoming transport connections for which the ATN Security Label is inappropriate. Again, the mechanism for determining the ATN Security Label associated with an incoming transport connection is a local matter.

2.7.3.2 In the Connectionless Mode

In the connectionless mode, unless used to convey General Communications data, each incoming or outgoing TSDU shall be associated with an ATN Security Label. For outgoing TSDUs, this ATN Security Label shall be encoded into the header of the resulting NPDU. For incoming TSDUs, the associated ATN Security Label shall be the ATN Security Label that was encoded into the header of the incoming NPDU that contained the TSDU.

Note. — The mechanism by which ATN Security Labels are associated with TSDUs is a local matter.

2.7.4 Network Layer Security

2.7.4.1 Service Provider to the Transport Layer

The Network Service shall provide a mechanism that permits an ATN Security Label to be associated with an NSDU:

a) When passed from the transport layer to the network layer in an NS-UNITDATA.req. This ATN Security Label shall be encoded into the corresponding CLNP NPDU header(s) according to section 6.2.2.1.

b) When passed from the network layer to the transport layer in an NS-UNITDATA.ind. This ATN Security Label shall be that received in the associated CLNP NPDU header(s).

2.7.4.2 Routing Control

When present in an NPDU header, the network layer routing functions shall ensure that:

a) The User Routing Policy requirements, if any, encoded into the ATN Security Label are obeyed, and

b) The NPDU is only routed over paths through the internetwork which both permit and are suitable for data of the traffic type identified by the ATN Security Label.

Note 1. — Section 3.2.1 specifies the forwarding procedures that ensure the above.

Note 2. — The Security Information conveyed in IDRP routes is used to provide the forwarding

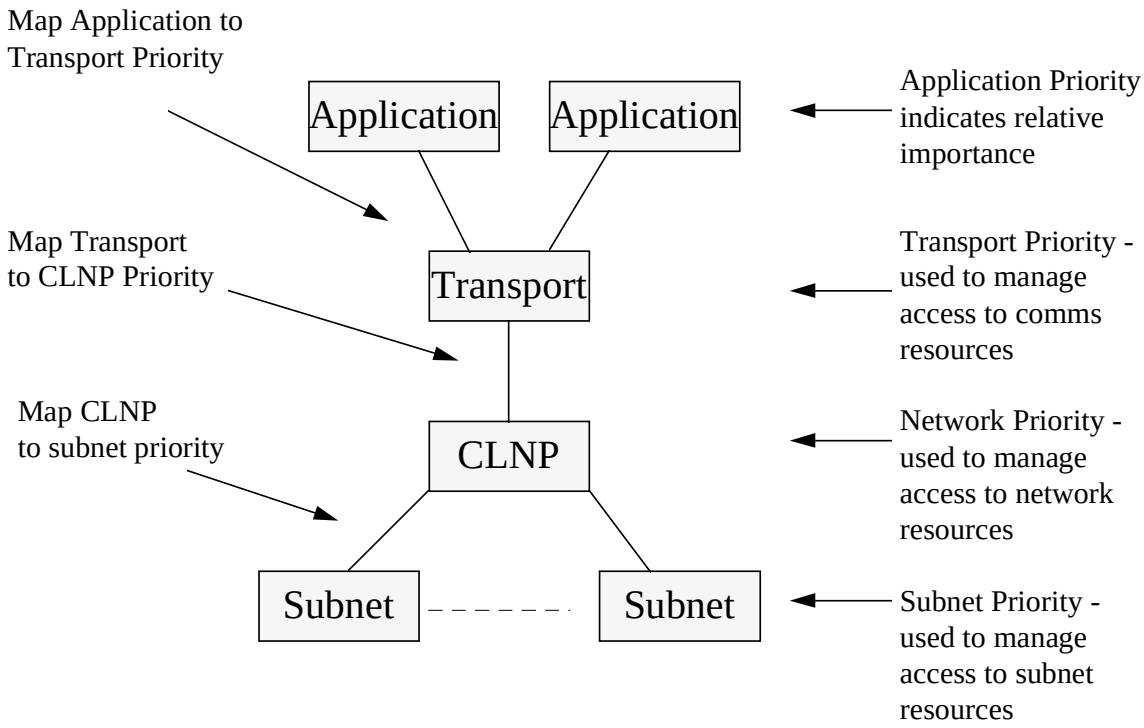


Figure 2-2 Use of Priority in the ATN

process with the information needed to support the above.

2.7.4.3 Protection of the Routing Information Base

IDRP type 1 Authentication shall be used as a mechanism for ensuring the integrity of routing information exchange by IDRP.

Note. — A later extension to support type 2 authentication will enable the routing information base to be protected from attackers that try to modify routing information while in transit, or which attempt to masquerade as genuine ATN Routers.

2.7.5 Subnetwork Provisions

Note. — There are no requirements for security mechanisms in ATN Subnetworks. However, Administrations and other Organisations implementing ATN subnetworks are encouraged to ensure the general security and availability of ATN subnetworks through the use of physical security mechanisms.

2.8 ATN Use of Priority

Note 1. — The purpose of priority is to signal the relative importance and/or precedence of data, such that when a decision has to be made as to which data to action first, or when contention for access to shared resources has to be resolved, the decision or outcome can be determined unambiguously and in line with user requirements both within and between applications.

Note 2. — In the ATN, priority is signalled separately by the application in the transport layer and network layer, and in ATN subnetworks. In each case, the semantics and use of priority may differ. ***Figure 2-2*** *illustrates where priority is applied in the ATN, and where it is necessary to map the semantics and syntax of ATN priorities*

Note 3. — In the ATN Internet, priority has the essential role of ensuring that high priority safety related data is not delayed by low priority non-safety data, even when the network is overloaded with low priority data.

2.8.1 Application Priority

Note 1. — Priority in ATN Application Protocols is used to distinguish the relative importance and urgency of application messages within the context of that application alone.

For the purpose of

a) distinguishing the relative importance and urgency of messages exchanged by different ATN Applications, and

b) distinguishing the relative importance and urgency of messages of the same application during their transit through the ATN,

application messages shall be grouped into one or more categories listed in Table 2-1.

Note 2. — An ATN Application may include messages from more than one category.

When a message is sent between ATN Application Entities, the message shall be sent using either:

a) a transport connection established using the Transport Connection Priority listed in Table 2-3 for the message's message category, or

b) the connectionless transport service, signalling the Connectionless Transport Service Priority listed in Table 2-3 for the message's message category.

Note 3. — The priority of an individual transport connection cannot be changed during the lifetime of the connection. Therefore, if an application exchanges messages belonging to more than one message category using the connection mode transport service, then a separate transport connection needs to be established for each message category.

2.8.2 Transport Connection Priority

Note 1. — Transport priority is concerned with the relationship between transport connections and determines the relative importance of a transport connection with respect to (a) the order in which TCs are to have their QoS degraded, if necessary, and (b) the order in which TCs are to be broken in order to recover resources.

Note 2. — The transport connection priority is specified by the transport user either explicitly or implicitly, when the transport connection is established.

When an ATN Transport Layer entity is unable to satisfy a request for a transport connection from either a local or remote TSAP, and which is due to insufficient local resources available to the transport layer entity, then it shall terminate a lower priority transport connection, if any, in order to permit the establishment of a new higher priority transport connection.

Note 3. — Implementations may also use transport priority to arbitrate access to other resources (e.g. buffers). For example, this may be achieved by flow control applied to local users, by discarding received but unacknowledged TPDUs, by reducing credit windows, etc.

All TPDUs sent by an ATN Transport Layer Entity shall be transferred by the ATN Internet Layer, using the Network Protocol Priority that corresponds to the transport connection's priority according to Table 2-3.

2.8.3 Connectionless Transport Service Priority

Note 1. — There are no procedures required of the ATN Connectionless Transport Entity in respect of priority, except for mapping the TSDU priority supplied by the service user (i.e. an ATN Application), to the corresponding Network Layer Priority, and vice versa.

All UD TPDUs sent by an ATN Transport Layer Entity shall be transferred by the ATN Internet Layer using the Network Protocol Priority that corresponds to the TSDU priority provided by the service user according to Table 2-3

2.8.4 ATN Internet Priority

Note 1. — In the ATN Internet Layer, an NPDU of a higher priority is given preferred access to resources. During periods of higher network utilisation, higher priority NPDUs may therefore be expected to be more likely to reach their destination (i.e. are less likely to be discarded by a congested router) and to have a lower transit delay (i.e. be more likely to be selected for transmission from an outgoing queue) than are lower priority packets.

ATN Internet Entities shall maintain their queues of outgoing NPDUs in strict priority order, such

that a higher priority NPDU in an outgoing queue will always be selected for transmission in preference to a lower priority NPDU.

Note 2. —priority zero is the lowest priority.

During periods of congestion, or when any other need arises to discard NPDUs currently held by an ATN Internet Entity, lower priority NPDUs shall always be discarded before higher priority NPDUs.

Note 3. — In addition to NPDUs containing user (i.e. transport layer) data, the Internet Layer also forwards routing information contained in CLNP Data PDUs (e.g. IDRP) and as distinct NPDUs (e.g. ES-IS). These must all be handled at the highest priority if changes to network topology are to be quickly actioned and the optimal service provided to users.

BISPDUs exchanged by IDRP shall be considered as Network/Systems Management category messages, and sent using CLNP priority 14.

ES-IS (ISO 9542) PDUs shall be implicitly assumed to have priority 14 and shall be forwarded as if they were CLNP PDUs of priority 14.

Note 4. — The priority encoded in an ISH PDU conveys the priority of the sending system, and not the priority of the PDU.

2.8.5 ATN Subnetwork Priority

2.8.5.1 Connection Mode Subnetworks

Note 1. — In a connection mode ATN subnetwork, priority is used to distinguish the relative importance of different data streams (i.e. the data on a subnetworks connection), with respect to gaining access to communications resources and to maintaining the requested Quality of Service.

Note 2. — On some subnetworks (e.g. public data networks), not all data streams will be carrying ATN messages. Therefore, subnetwork priority is also used to distinguish ATN and non-ATN data streams.

Note 3. — So as not to incur the overhead and cost of maintaining too many simultaneous subnetwork connections, NPDUs of a range of Network Layer priorities may be sent over the same subnetwork connection.

When an ATN connection mode subnetwork does not support prioritisation of subnetwork connections, then the ATN Internet Entity shall not attempt to specify a subnetwork connection priority, and NPDUs of any priority may be sent over the same subnetwork connection.

Note 4. — The following does not apply to AMSS and Mode S Subnetworks, which have specified their own priority mapping schemes.

When an ATN connection mode subnetwork does support prioritisation of subnetwork connections, then unless the relationship between ATN Internet Priority and subnetwork priority is explicitly specified by the subnetwork specification, the following shall apply:

a) Subnetwork connections shall be established as either “High” or “Low” priority connections.

b) For the “Low” priority connection type, the priority to gain a connection, keep a connection and for data on the connection shall be the defaults for routine use of the subnetwork.

c) For the “High” priority connection type, the priority to gain a connection, keep a connection and for data on the connection shall be appropriate for urgent and network management data in the context of the subnetwork, In the absence of guidance from the subnetwork provider, the value decimal 8 shall be used for each of the three priorities.

d) “High” priority connections shall be used to convey NPDUs of priority six and above. “Low” priority connections shall be used to convey all other NPDUs.

When a subnetwork connection is established between two ATN Internet Entities and no subnetwork connection between these two entities exists over any subnetwork, then that subnetwork connection shall always be established at a priority suitable for conveying priority 14 NPDUs (i.e. Network/Systems Management).

Note 5. — This is to ensure that routing information can be exchanged at the appropriate priority.

2.8.5.2 Connectionless Subnetworks

Note 1. — The purpose of priority on a connectionless subnetwork is to provide higher priority NPDUs with preferred access to subnetwork resources.

Note 2. — The relationship between NPDU priority and subnetwork priority is subnetwork specific.

Message Categories	**Corresponding Protocol Priority**		
	Transport Layer Priority		**Internet Layer Priority**
	Transport Connection Priority	**TSDU Priority**	**CLNP Priority**
Network/Systems Management	0	0	14
Distress Communications	1	1	13
Urgent Communications	2	2	12
High Priority Flight Safety Messages	3	3	11
Normal Priority Flight Safety Messages	4	4	10
Meteorological Communications	5	5	9
Flight Regularity Communications	6	6	8
Aeronautical Information Service Messages	7	7	7
Network/Systems Administration	8	8	6
Aeronautical Administrative Messages	9	9	5
<unassigned>	10	10	4
Urgent Priority Administrative and U.N. Charter Communications	11	11	3
High Priority Administrative and State/Government Communications	12	12	2
Normal Priority Administrative	13	13	1
Low Priority Administrative	14	14	0

Table 2-3 Relationship of Communication priorities in the ATN

When an NPDU is sent over a connectionless ATN Subnetwork which supports data prioritisation, the subnetwork priority assigned to the transmitted packet shall be that specified by the subnetwork provider as corresponding to the NPDU priority.

3. ATN ROUTING

3.1 Introduction

3.1.1 Scope

This chapter provides requirements and recommendations pertaining to the deployment of ATN components within the ATN Internet; use of routing information distributed according to ISO/IEC 10747 in order to support policy based and mobile routing in the Aeronautical Telecommunications Network; and the Route Initiation procedures for initiating the exchange of routing information using the ISO/IEC 10747 protocol. In the case of air-ground data links, route initiation also includes the use of the ISO/IEC 9542 protocol. This chapter is not concerned with compliancy with the ISO/IEC 10747 and ISO/IEC 9542 protocols. This is the subject of chapter 8.

3.1.2 Applicability of Requirements

Note 1.— The classes of ATN Router referred to below are defined in 2.4.

Note 2.— The ATN RDs referred to below are defined in 2.2.

ATN Ground-Ground Routers shall comply with the provisions of 3.4 and 3.6. When used as an ATN Router in an ATN RD that is a member of an ATN Island Backbone RDC, an ATN Ground-Ground Router shall also comply with the provisions of 3.7.1. When used in any other ATN Transit Routing Domain, an ATN Ground-Ground Router shall also comply with the provisions of 3.7.3. Otherwise, an ATN Ground-Ground Router shall comply with the provisions of 3.7.4.

ATN Air/Ground Routers shall comply with the provisions of 3.4 for ground-ground interconnection, 3.5 for air/ground interconnection and 3.6. When used as an ATN Router in an ATN RD that is a member of an ATN Island Backbone RDC, an ATN Air/Ground Router shall also comply with the provisions of 3.7.1. When used in any other ATN Transit Routing Domain, an ATN Air/Ground Router shall also comply with the provisions of 3.7.3.

ATN Airborne Routers shall comply with the provisions of 3.5, 3.6, and 3.7.2.

When an RD is declared to be an ATN RD then it shall comply with the provisions of 2.2.2.

When an RD is declared to be a Mobile RD, then it shall comply with the provisions 2.2.2.3.

When an RDC is declared to be an ATN Island RDC then its member RDs shall comply with the provisions of 2.2.3.1.

When an RDC is declared to be an ATN Island Backbone RDC then its member RDs shall comply with the provisions of 2.2.4.1.

3.2 Service Provided by an ATN Routing Domain

Note 1.— An ATN Routing Domain may operate as an ATN Service Provider, in which case it operates as a Transit Routing Domain and offers routes to other ATN RDs.

Note 2.— an ATN RD may also be considered as providing the facilities of an ATN Service Provider when offering routes to destinations within itself.

A route shall only be advertised by an ATN Service Provider to an adjacent ATN RD when it can be ensured that data sent over that route by the RD to which the route is advertised, is acceptable to every RD and RDC in the route's path, and will be relayed by them to the route's destination.

Note 3.— The acceptability of a route may be determined using a priori knowledge derived from interconnection agreements with other RDs.

An ATN RD shall only forward a CLNP NPDU to an ATN Service Provider when that ATN Service Provider is advertising a route to the NPDU's destination, and the route is defined below as being a route over which the ATN Service Provider is required to forward the NPDU.

3.2.1 Forwarding CLNP NPDUs

Note 1.— Forwarding decisions that also take into account the CLNP QoS Maintenance Parameter are a local matter and an ATN Service Provider may hence ignore this parameter.

3.2.1.1 Forwarding a CLNP NPDU when no Security Parameter is present in the PDU Header

When a CLNP NPDU is received by an ATN Service Provider and that NPDU does not contain a Security Parameter in the PDU Header then that NPDU shall be forwarded over the route, if present, that either:

1. contains a security path attribute comprising the ATN Security Registration Identifier and security information that comprises:
   a) either an Air/Ground Subnetwork Security Tag that has "ATN General Communications" in its set of permissible Traffic Types, or
   b) no Air/Ground Subnetwork Security Tag, or
2. does not contain any security path attribute.

If no such route can be found then the NPDU shall be discarded.

3.2.1.2 Forwarding a CLNP NPDU when a Security Parameter is present in the PDU Header

When a CLNP NPDU is received by an ATN Service Provider and that NPDU contains a Security Parameter in the Globally Unique Format, and encodes security related information according to Chapter 6 under the ATN Security Registration Identifier, then the NPDU shall be forwarded according to the procedures specified below.

Note 1. — The CLNP Header Security Parameter is used to indicate the Traffic Type of the application data contained in the NPDU, and the application's routing policy requirements.

Note 2.— The procedures for handling an NPDU with any other format of Security Parameter, or with any other Security Registration Identifier are outside the scope of this specification.

3.2.1.2.1 ATN Operational Communications - ATSC Traffic Type

3.2.1.2.1.1 No Routing Policy Specified

Note 1.— This case corresponds to a Traffic Type and Associated Routing Policy Security Tag value of 000 00001.

If the NPDU contains a CLNP Header Security Parameter in the globally unique format, and encodes:

a) security related information according to Chapter 6 under the ATN Security Registration Identifier,
b) a traffic type of ATN Operational Communications - Air Traffic Service Communications, and
c) no Routing Policy Specified,

then the NPDU shall be forwarded over a selected route to the NPDU's destination that contains a security path attribute comprising the ATN Security Registration Identifier and security information that comprises:

i. An Air/Ground Subnetwork Security Tag that has "ATN Operational Communications - Air Traffic Services Communications" in its set of permissible Traffic Types, or
ii. no Air/Ground subnetwork Security Tag, and
I. no ATSC Class Security Tag, or,
II. if no such route is present, then an ATSC Class Security Tag indicating support of the lowest class out of all such routes available.

Note 2.— ATSC Class "H" is the lowest and Class "A" is the highest.

If no such route can be found then the NPDU shall be discarded.

3.2.1.2.1.2 ATSC Class Specified

Note 1.— This case corresponds to Traffic Type and Associated Routing Policy Security Tag values 000 10000 to 000 10111 inclusive.

If the NPDU contains a CLNP Header Security Parameter in the globally unique format, and encodes:

a) security related information according to Chapter 6 under the ATN Security Registration Identifier,
b) a traffic type of ATN Operational Communications - Air Traffic Service Communications, and
c) a requirement to route the NPDU over a route of a specified ATSC Class,

then the NPDU shall be forwarded over a selected route to the NPDU's destination that contains a security path attribute comprising the ATN Security Registration Identifier and security information that comprises:

i. An Air/Ground Subnetwork Security Tag that has "ATN Operational Communications - Air Traffic Services Communications" in its set of permissible Traffic Types, or
ii. no Air/Ground Subnetwork Security Tag

and,

an ATSC Class Security Tag indicating support of the required class, or a higher class.

Note 2.— ATSC Class "H" is the lowest and Class "A" is the highest.

If no such route can be found then the NPDU shall be discarded.

If multiple routes are available which meet or exceed the required ATSC Class, then the route with the lowest relative cost shall be selected.

3.2.1.2.2 Air-Ground Subnetwork Preference Specified

Note 1. — This case corresponds to Traffic Type and Associated Routing Policy Security Tag value 000 00011.

If the NPDU contains a CLNP Header Security Parameter in the globally unique format, and encodes:

a) security related information according to chapter 6 under the ATN Security Registration Identifier,

b) a traffic type of ATN Operational Communications - Air Traffic Service Communications, and

c) a requirement to route the NPDU over a specific Air-Ground subnetwork type, with an ordered preference of Mode S first, then VHF Data Link, then Satellite Data Link, then HF Data Link,

then the NPDU shall be forwarded over a selected route to the NPDU's destination that contains a security path attribute comprising the ATN Security Registration Identifier and security information that comprises no ATSC Class Security Tag, or, if no such route is present, then an ATSC Class Security Tag indicating the lowest class out of all such routes available, and an Air/Ground Subnetwork Security Tag that indicates:

i. that the route passes over a Mode S Subnetwork and has "ATN Operational Communications - Air Traffic Services Communications" in its set of permissible Traffic Types, or,

ii. if such a route does not exist, then such a route that indicates that the route passes over a VDL Subnetwork and has "ATN Operational Communications - Air Traffic Services Communications" in its set of permissible Traffic Types, or,

iii. if such a route does not exist, then such a route that indicates that the route passes over a Satellite Subnetwork and has "ATN Operational Communications - Air Traffic Services Communications" in its set of permissible Traffic Types, or,

iv. if such a route does not exist, then such a route that indicates that the route passes over an HF Subnetwork and has "ATN Operational Communications - Air Traffic Services Communications" in its set of permissible Traffic Types, or,

v. if such a route does not exist then a route without an Air/Ground Subnetwork Security Tag, or

vi. if such a route does not exist then the NPDU shall be discarded.

If after applying the above procedures, a more specific route is available to the NPDU's destination, but

1) the route has an Air/Ground Subnetwork Security Tag that indicates that the route passes over a lower preference Air/Ground Subnetwork while

2) having "ATN Operational Communications - Air Traffic Service Communications" in its set of permissible Traffic Types, then

3) the more specific route shall be selected in preference to the less specific route.

Note 3.— The purpose of this requirement is to ensure that the NPDU is not forced to visit a default route provider only to find that a higher preference route does not actually exist to the NPDU's destination.

3.2.1.2.3 ATN Operational Communications - AOC Traffic Type

3.2.1.2.3.1 No Routing Policy Specified

Note 1.— This case corresponds to a Traffic Type and Associated Routing Policy Security Tag value of 001 00001.

If the NPDU contains a CLNP Header Security Parameter in the globally unique format, and encodes:

a) security related information according to Chapter 6 under the ATN Security Registration Identifier,

b) a traffic type of ATN Operational Communications - Aeronautical Operational Control, and

c) no Routing Policy Specified,

then the NPDU shall be forwarded over a selected route to the NPDU's destination that contains a security path attribute comprising the ATN

Security Registration Identifier and security information that comprises:

i. an Air/Ground Subnetwork Security Tag that has "ATN Operational Communications - Aeronautical Operational Control" in its set of permissible Traffic Types, or

ii. no Air/Ground Subnetwork Security Tag.

If no such route can be found then the NPDU shall be discarded.

3.2.1.2.3.2 Air/Ground Subnetwork Type Specified

Note 1.— This case corresponds to Traffic Type and Associated Routing Policy Security Tag values 001 00010 through to 001 00110, inclusive.

Note 2.— The Air/Ground Subnetworks that may be so specified are: Gatelink, VDL, AMSS, HF and Mode S.

If the NPDU contains a CLNP Header Security Parameter in the globally unique format, and encodes:

a) security related information according to Chapter 6 under the ATN Security Registration Identifier,

b) a traffic type of ATN Operational Communications - Aeronautical Operational Control, and

c) a requirement to route traffic only via a specific Air/Ground Subnetwork only,

then the NPDU shall be forwarded over a selected route to the NPDU's destination that contains a security path attribute comprising the ATN Security Registration Identifier and security information that comprises either

i. an Air/Ground Subnetwork Security Tag that indicates that the route passes over that Air/Ground Subnetwork and has "ATN Operational Communications - Aeronautical Operational Control" in its set of permissible Traffic Types, or,

ii. no Air/Ground Subnetwork Security Tag.

If no such route can be found then the NPDU shall be discarded.

3.2.1.2.3.3 Air/Ground Subnetwork Order of Preference Specified

Note 1.— This case corresponds to Traffic Type and Associated Routing Policy Security Tag values 001 00111 through to 001 01001, inclusive.

Note 2.— The Air/Ground Subnetworks for which an order of preference may be so specified are: Gatelink, VDL, AMSS, HF and Mode S.

If the NPDU contains a CLNP Header Security Parameter in the globally unique format, and encodes:

a) security related information according to Chapter 6 under the ATN Security Registration Identifier,

b) a traffic type of ATN Operational Communications - Aeronautical Operational Control, and

c) a requirement to route traffic only via certain Air/Ground Subnetworks and with a specified order of preference,

then the NPDU shall be forwarded over a selected route to the NPDU's destination that contains a security path attribute comprising the ATN Security Registration Identifier and security information that comprises:

i. an Air/Ground Subnetwork Security Tag that indicates that the route passes over the first preference Air/Ground Subnetwork and has "ATN Operational Communications - Aeronautical Operational Control" in its set of permissible Traffic Types, if present, or

ii. an Air/Ground Subnetwork Security Tag that indicates that the route passes over the second preference Air/Ground Subnetwork and has "ATN Operational Communications - Aeronautical Operational Control" in its set of permissible Traffic Types, if present, and so on until a suitable route is found or no further preferences are specified, or

iii. no Air/Ground Subnetwork Security Tag.

If no route can be found then the NPDU shall be discarded.

If after applying the above procedures, a more specific route is available to the NPDU's destination, but

1) the route has an Air/Ground Subnetwork Security Tag that indicates that the route passes over a lower preference Air/Ground Subnetwork while

2) having "ATN Operational Communications - Aeronautical Operational Control" in its set of permissible Traffic Types, then

3) the more specific route shall be selected in preference to the less specific route.

Note 3.— The purpose of this requirement is to ensure that the NPDU is not forced to visit a default route provider only to find that a higher preference route does not actually exist to the NPDU's destination.

3.2.1.2.4 ATN Administrative Communications Traffic Type

Note 1.— This case corresponds to a Traffic Type and Associated Routing Policy Security Tag value of 001 10000.

If the NPDU contains a CLNP Header Security Parameter in the globally unique format, and encodes:

a) security related information according to Chapter 6 under the ATN Security Registration Identifier,

b) a traffic type of ATN Administrative Communications,

then the NPDU shall be forwarded over a selected route to the NPDU's destination that contains a security path attribute comprising the ATN Security Registration Identifier and security information that comprises:

i. either an Air/Ground Subnetwork Security Tag that has "ATN Administrative Communications" in its set of permissible Traffic Types, or

ii. no Air/Ground Subnetwork Security Tag.

If no such route can be found then the NPDU shall be discarded.

3.2.1.2.5 ATN Systems Management Communications Traffic Type

Note 1.— This case corresponds to a Traffic Type and Associated Routing Policy Security Tag value of 011 00000.

If the NPDU contains a CLNP Header Security Parameter in the globally unique format, and encodes:

a) security related information according to Chapter 6 under the ATN Security Registration Identifier,

b) a traffic type of ATN Systems Management Communications,

then the NPDU shall be forwarded over a selected route to the NPDU's destination that:

1. contains a security path attribute comprising the ATN Security Registration Identifier and security information that comprises:

    a) either an Air/Ground Subnetwork Security Tag that has "ATN Systems Management Communications" in its set of permissible Traffic Types, or

    b) no Air/Ground Subnetwork Security Tag, or

2. no security path attribute.

If no such route can be found then the NPDU shall be discarded.

3.3 The Deployment of ATN Components

3.3.1 Interconnection of ATN RDs

ATN RDs shall be interconnected by real subnetworks permitting communication between ATN Routers for each of the interconnection scenarios specified below.

Note 1.— Examples of possible interconnections between ATN Routing Domains are illustrated in Figure 2-1.

Note 2.— There is no requirement for all ATN RDs to be fully interconnected.

Except for the interconnection of Mobile RDs with other ATN RDs, the real subnetwork used for such an interconnection shall be chosen by bilateral agreement and may be any subnetwork that can be used to convey the ISO 8473 protocol and provides the required quality of service.

Note 3.— For example, the chosen subnetwork may be a point-to-point communications link, a public or private PSDN providing the CCITT X.25 network access service, an Ethernet or an ISDN, etc.

Note 4.— The Dynamic procedures for the interconnection of two ground based ATN Routers are specified in 3.4, and for interconnection of an Air/Ground and an Airborne Router in 3.5. The remainder of this section is concerned with static interconnection requirements.

3.3.1.1 Interconnection between Members of an ATN Island Backbone RDC

When there is more than one ATN RD in an ATN Island Backbone RDC, each Administration or Aeronautical Industry Member that has elected to participate in that ATN Island's Backbone RDC, shall ensure that its RD is either:

a) interconnected directly with all other ATN RDs within the ATN Island's Backbone RDC, over a suitable and mutually agreeable real subnetwork or

b) interconnected directly as above, with one or more ATN RDs that are also members of the ATN Island's Backbone RDC, and which are able and willing to provide routes to the remaining RDs within the Backbone RDC.

Note.— The existence of the ATN Backbone RDC prohibits routes between its member RDs via other ATN RDs in the same ATN Island.

3.3.1.2 Interconnection between Members of an ATN Island Backbone RDC and other ATN RDs within the ATN Island

ATN RDs within an ATN Island RDC that are not members of the ATN Island's Backbone RDC, shall ensure that they are either:

a) interconnected directly with one or more ATN RDs that are members of the ATN Island's Backbone RDC, over suitable and mutually agreeable real subnetworks; or

b) interconnected with one or more other ATN RDs that are members of the same ATN Island RDC and which are able and willing to provide routes to and from one or more ATN RDs within the same ATN Island's Backbone RDC, and to all destinations reachable via the ATN Island's Backbone.

3.3.1.3 Interconnection of ATN Islands

ATN Islands shall only interconnect via ATN RDs which are members of each ATN Island's Backbone RDC.

When an ATN RD is a member of more than one ATN Island RDC, its routing policy shall not permit it to operate as a TRD between sources and destinations in different ATN Islands unless the RD is a member of each island's Backbone RDC.

3.3.1.4 Interconnection of Mobile and Fixed RDs

Note 1.— A Mobile RD may interconnect concurrently with multiple ATN RDs which are attached to the mobile subnetworks and which are accessible to the Mobile RD at any given time. The purpose of such interconnections is to provide data link communications services when required by CNS/ATM applications and other aeronautical or airline industry applications.

In order to meet the availability requirements of CNS/ATM applications, Airborne and Air/Ground Routers shall be capable of supporting multiple concurrent adjacencies with other Routers; these adjacencies are supported by multiple subnetwork connections at the same or different priorities, using the same or different air/ground subnetworks.

Note 2. — Dynamically, such adjacencies may be established and released in a « make before break » fashion permitting continuous communications availability, and for the suitability of a newly available adjacency to be determined before a no longer needed adjacency is released.

Note 3. — It is not within the scope of this specification to set minimum requirements in respect of the number of adjacencies and subnetwork connections that an Airborne or Air/Ground Router must support. Such requirements are dependant on the published coverage and number of air/ground subnetworks, application availability requirements and additionally, in the case of Airborne Routers, on Airline operating policies. Implementors are advised to interpret « multiple » as, in the context of the above requirement, implying at least two adjacencies or connections, and, in practice, a larger number is anticipated as being the likely minimum requirement.

3.3.1.5 Interconnection of ATN RDs and non-ATN RDs

Note.— ATN RDs may interconnect with non-ATN RDs whether they are members of the same Administrative Domain or not.

3.4 Ground-Ground Interconnection

3.4.1 Interconnection Scenarios

Note 1.— Ground-Ground interconnection procedures apply to the interconnection of two Ground-Ground Routers, and to the interconnection of an Air/Ground Router and a Ground-Ground Router.

Note 2.— Formally, these procedures only apply to interconnection between ATN Routers in different Administrative Domains. However, in practice, they are also applicable to interconnection scenarios within the same Administrative Domain.

3.4.2 Ground-Ground Route Initiation

Note 1.— Route Initiation is defined to be the point at which routing information exchange can begin, and the route initiation procedures are those that permit the exchange of routing information to commence.

When the Network Administrators agree to the Ground-Ground interconnection of one or more ATN Routers within their Administrative Domains, they shall:

a) Make available suitable subnetwork connectivity including, where necessary the physical installation of suitable communications equipment for end-to-end communications between the ATN Routers, and supporting the Quality of Service necessary for the applications data that will be routed over this interconnection.

Note 2.— The choice of appropriate subnetwork(s) to support the interconnection is a matter for bilateral agreement between network administrators, including agreement on responsibility for installation, operating and maintenance costs, and fault management.

b) Using global or local Systems Management mechanisms, establish one or more subnetwork connections between the two ATN Routers, unless the subnetwork technology is connectionless when this step may be omitted.

Note 3.— Typically (e.g. with X.25), one ATN Router will be placed in a state where it will accept an incoming connection from the other ATN Router, and then the other ATN Router is stimulated to initiate one or more subnetwork connection(s) to the other ATN Router.

Note 4.— Multiple concurrent subnetwork connections over the same or different subnetworks may be required in order to meet throughput and other QoS requirements.

c) Using global or local Systems Management mechanisms, ensure that the forwarding information base in each ATN Router, used to support the connectionless network protocol specified in Chapter 6, contains sufficient information to forward CLNP NPDUs addressed to the NET of the other ATN Router, over the newly established subnetwork connection(s).

Note 5.— This step is necessary to ensure that the connectionless network service can be used to exchange the BISPDUs of IDRP.

d) Using global or local Systems Management mechanisms:

i) append the NET of the remote ATN Router to the **externalBISNeighbor** attribute of the BIS's **idrpConfig** MO,

ii) create an **AdjacentBIS** Managed Object (MO) in each ATN Router to represent the other ATN Router, and

iii) invoke the start event action on each such MO, in order to initiate a BIS-BIS connection between the two ATN Routers.

*Note 6.— As a matter for the bilateral agreement of the Network Administrators, either (a) both ATN Routers will attempt to open the BIS-BIS connection using the active open procedures, that is with the **ListenForOpen** MO attribute set to false, or (b) one and only one sets this attribute to true.*

3.4.3 Ground-Ground Routing Information Exchange

Routing information shall be exchanged using the ISO/IEC 10747 Inter-Domain Routing Protocol according to the profile specified in Chapter 8. In support of Air/Ground communications, the exchange of routing information shall be subject to appropriate routing policies specified in 3.7.1, 3.7.3, or 3.7.4, depending upon the role of the Routing Domain in which each ATN Router is located.

3.4.4 Ground-Ground Route Termination

Note 1.— Route Termination is defined to be the point at which routing information ceases to be exchanged between two ATN Routers, and, in consequence, the routes made available over the adjacency cease to be useable and must be withdrawn. The route termination procedures are those procedures which terminate the exchange of routing information.

Note 2.— Route Termination may result from a failure in the underlying subnetworks causing a loss of communication between the two ATN Routers. Alternatively, it may result from a deliberate decision of Network Administrators to terminate the interconnection, either temporarily or permanently.

Note 3.— No special recovery procedures are specified if route termination is due to a network fault. Once the fault has been repaired, the procedures of 3.4.2 are re-invoked, as appropriate to re-establish communication, and to exchange routing information.

When a Network Administrator decides to temporarily or permanently terminate an interconnection between two ATN Routers then, using global or local Systems Management mechanisms applied to either or both of the two ATN Routers, the **deactivate** action shall be invoked on the **AdjacentBIS** MO that represents the remote ATN Router with which the BIS-BIS connection is to be terminated.

If the adjacency is to be permanently terminated, then the **AdjacentBIS** MO shall also be deleted, and the forwarding information base shall be updated to remove the route to the NET of the remote ATN Router.

For either temporary or permanent termination, and if required, by using global or local Systems Management mechanisms, the Network Administrator(s) shall also terminate the underlying subnetwork connections.

3.5 Air-Ground Interconnection

3.5.1 Interconnection Scenarios

Note 1.— Air-Ground interconnection applies to the interconnection between an ATN Airborne Router and an ATN Air/Ground Router over one or more mobile subnetworks.

Note 2.— The significant difference between Air-Ground and Ground-Ground Interconnection is that in the former case interconnection is automatic and consequential on the availability of communications and local policy, while, in the latter case, interconnection is a deliberate and planned action with the direct involvement of Network Administrators.

Note 3.— While IDRP is also intended to be used over Air-Ground Interconnections, as an interim measure, the optional non-use of IDRP over Air-Ground Interconnections is permitted by this specification and according to 3.5.2.11.

Note 4.— For the purposes of this specification, the functional model of a Router illustrated in Figure 3-1 is assumed. This model illustrates the basic functional entities in a router, the data flow between them as thick lines, and the flow of certain events and control information, by dashed lines.

Note 5.— Figure 3-1 introduces a new architectural entity, the Intermediate System - Systems Management Entity (IS-SME). As specified below, this plays an important role in the realisation of Route Initiation in Air/Ground Operations, by responding to changes in subnetwork connectivity and thereby controlling the route initiation and termination procedures.

3.5.2 Air-Ground Route Initiation

BIS-BIS communications over a mobile subnetwork shall be either air-initiated or ground-initiated, with one of these two modes of operation selected for all instances of a given subnetwork type.

Note 1.— Three classes of procedure are distinguished by this specification. These are: (a) Air Initiated i.e. when the Airborne Router initiates the procedure, (b) Ground Initiated i.e. when the Air/Ground Router initiates the procedure, and (c) Air or Ground Initiated i.e. when either the Airborne or the Air/Ground Router may initiate the procedure.

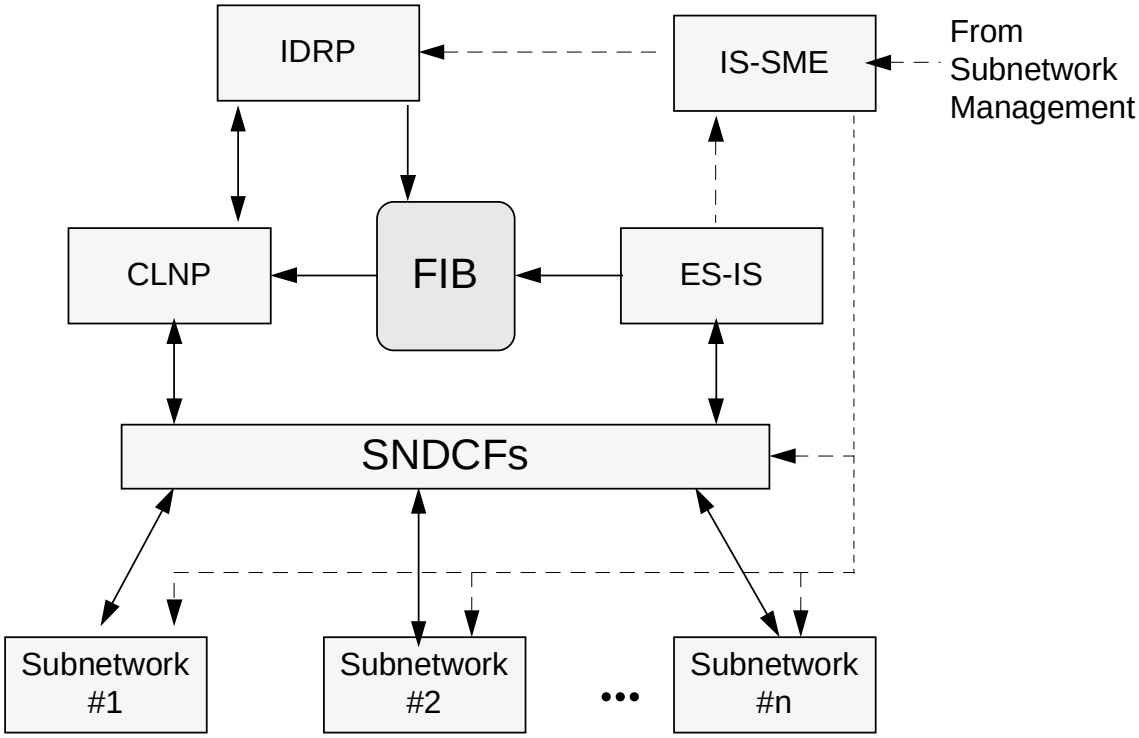


Figure 3-1 Assumed ATN Router Architecture for Air/Ground Route Initiation

Note 2.— Two types of mobile subnetworks are also recognised by this specification. These are: (a) those which provide information on the availability of specific mobile systems on the subnetwork through the Join Event defined in this section, and (b) those which do not. The latter type are only appropriate to Route Initiation Procedures which are Air Initiated.

Note 3.— For a given mobile subnetwork type, the use of air-initiated or ground-initiated procedures, and the implementation of Join Events is outside of the scope of this specification, and is a matter for the SARPs specified by the relevant ICAO panel.

Note 4.— The interfaces to all mobile subnetworks are assumed to be compatible with ISO 8208. The ISO 8208 term DTE is also used in this specification to refer to a system attached to a mobile subnetwork,

For Air-Initiated Subnetworks that do not provide information on the availability of specific mobile systems, Airborne Routers shall comply with the procedures specified in 3.5.2.2.1, and Air/Ground Routers shall comply with the procedure specified in 3.5.2.1.

For Air-Initiated Subnetworks that do provide information on the availability of specific mobile systems, Airborne Routers shall comply with the procedures specified in 3.5.2.2.2, and Air/Ground Routers shall comply with the procedure specified in 3.5.2.1.

For Ground-Initiated Subnetworks, Air/Ground Routers shall comply with the procedures specified in 3.5.2.3, and Airborne Routers shall comply with the procedure specified in 3.5.2.1.

For Air or Ground-Initiated Subnetworks, Air/Ground and Airborne Routers shall comply with the procedures specified in 3.5.2.1 and 3.5.2.4.

3.5.2.1 Route Initiation Procedures for a Responding ATN Router

Note 1.— Route Initiation is always asymmetric with a clearly defined initiator and responder. In all cases, the ATN Router in the responder role, follows the same procedures, as specified below.

Note 2.— For Air-Initiated Route Initiation, the Air/Ground Router is the responding ATN Router. For Ground-Initiated Route Initiation, the Airborne Router is the responding ATN Router.

Each ATN Router that is specified to take the responder role for a given Mobile Subnetwork type, and when attached to a subnetwork of that subnetwork type, shall be configured into a state whereby it "listens" for Call Indications on that subnetwork.

For each Call Indication received, a responding ATN Router shall either:

a) Accept the incoming call immediately using a Call Accept Packet

b) Validate the calling DTE and either accept the call using a Call Accept Packet, or if the call is unacceptable then it shall be rejected using a Clear Request Packet.

Note 3.— Whenever such a Call Indication is received the ATN Router validates the calling DTE and determines the acceptability of the call, using procedures outside the scope of this specification.

Note 4.— The number of simultaneous virtual circuits that the ATN Router needs to support will be subject to an implementation limit, that needs to be sufficient for the role in which the Router is deployed.

When a subnetwork connection is successfully established, then the procedures of 3.5.2.5 shall be applied to that subnetwork connection.

3.5.2.1.1 Emergency Use of a Mobile Subnetwork

In the case of Air Initiated Mobile Subnetworks, an Air/Ground Router shall not refuse a Call Indication or refuse to establish a BIS-BIS connection with an ATN Airborne Router, when a Call Indication from the ATN Airborne Router is received less than 5 minutes after a Call Indication was rejected, or a call terminated by Systems Management. The Air/Ground Router shall permit, through the implementation of an appropriate routing policy, the use of a so established connection for emergency and distress data.

Note 5. — This situation arises when the Airborne Router has no other air/ground connectivity, and refusal to accept a connection may cause a safety hazard. An Air/Ground Router may limit the use of such connections through routing policy, or permit full access, as a local matter.

3.5.2.2 Air-Initiated Route Initiation

3.5.2.2.1 Airborne Router Procedures for use of an ISO 8208 Mobile Subnetwork that does not Provide Information on Subnetwork Connectivity

An Airborne Router's IS-SME shall be configured with a list of subnetwork addresses for each mobile subnetwork of this type that it supports. This list should include the addresses which are necessary to meet the communication needs of the aircraft.

Note.— In the case of the AMSS, the Airborne Router's IS-SME will be configured with a list for each GES that the aircraft will use to communicate. Each such list will include the subnetwork addresses (e.g. DTEs) of the air/ground routers attached to the GES in question through which communications services may be required.

An Airborne Router's IS-SME shall continually issue a Call Request to each subnetwork address on each appropriate list with which it does not currently have a subnetwork connection and which is not subject to a back-off period (see 3.5.2.2.1.1), in turn. The period between each successive Call Request shall be configurable to ensure that the mobile subnetwork is not rendered unavailable.

When a subnetwork connection is successfully established, then the procedures of 3.5.2.5 shall be applied to that subnetwork connection. The polling procedure shall continue for the remaining subnetwork addresses on the list.

3.5.2.2.1.1 Call Request Failure

Whenever a Clear Indication is received in response to a Call Request that indicates rejection by the called DTE and includes a call clearing diagnostic code of 0, 133, 160..163, or 240, 241, 242, 244, 246, ..2489, then the Airborne Router shall implement a "back off" procedure. The back off procedure shall comprise the effective quarantining of the called subnetwork address for a period configurable on a per subnetwork basis from 5 minutes to 20 minutes. During this period, a Call Request shall not be issued to the subnetwork address.

The "back off" procedure shall not be started on receipt of a Clear Indication which includes any other call clearing diagnostic code.

If the call is cleared with a diagnostic code reporting an error that the SNDCF is unable to correct, then the called DTE shall be removed from the polled DTEs list. Otherwise, if required, the SNDCF shall retry the call after having resolved the cause of the call rejection.

Note 1. — Certain call clearing diagnostic codes in the range 128..143 are used by the Mobile SNDCF specified in chapter 7. The semantics of these codes is described ~~there~~ in table 7-6.

However, during any period when an Airborne Router does not have any subnetwork connections over mobile subnetworks, then all back off procedures shall be suspended until connectivity is established with at least one Air/Ground Router.

Note 2.— The purpose of the backoff procedure is to avoid unnecessarily overloading the network with Call Requests.

3.5.2.2.2 Airborne Router Procedures for use of an ISO 8208 Mobile Subnetwork that does Provide Connectivity Information

Note 1.— The connectivity information is provided as a "Join Event". This is an event generated by a mobile subnetwork when it is recognised that a system has attached to the subnetwork and is available for communication using the subnetwork. The Join Event provides the DTE Address of the newly available system.

Note 2.— An actual implementation of a Join Event may concatenate several distinct Join Events as defined above into a single message.

Note 3.— For air-initiated subnetworks, the Join Event is received by the IS-SME in the Airborne Router. The mechanism by which it is received is both subnetwork and implementation dependent.

On receipt of a Join Event, the Airborne Router shall either:

a) Issue an ISO 8208 Call Request with the DTE Address reported by the Join Event as the Called Address, or

b) Validate the DTE reported by the Join Event as to whether or not a subnetwork connection with it is acceptable according to local Routing Policy. If such a connection is acceptable then an ISO 8208 Call Request shall be issued with the DTE Address reported by the Join Event as the Called Address. Otherwise, the Join Event shall be ignored.

Note 4.— The Airborne Router validates the DTE that is the subject of the Join Event and determines the acceptability of a subnetwork connection with the so identified ATN Router, using procedures outside of the scope of this specification.

When a subnetwork connection is successfully established, then the procedures of 3.5.2.5 shall be applied to that subnetwork connection.

3.5.2.3 Ground-Initiated Route Initiation

Note 1.— Ground-Initiated Route Initiation is only appropriate for Mobile Subnetworks that originate a Join Event from their ground component.

Note 2.— For ground-initiated subnetworks, the Join Event is received by the IS-SME in the Air/Ground Router. The mechanism by which it is received is both subnetwork and implementation dependent.

On receipt of a Join Event, the Air/Ground Router shall either:

a) Issue an ISO 8208 Call Request with the DTE Address reported by the Join Event as the Called Address, or

b) Validate the DTE reported by the Join Event as to whether or not a subnetwork connection with it is acceptable according to local Routing Policy. If such a connection is acceptable then an ISO 8208 Call Request shall be issued with the DTE Address reported by the Join Event as the Called Address. Otherwise, the Join Event shall be ignored.

Note 3.— Option (b) above permits an administration or organisation operating a ground initiated mobile subnetwork to implement procedures, according to its local policy, whereby an Air/Ground Router may validate the DTE that is the subject of the Join Event and hence determine the acceptability of a subnetwork connection with the so identified Airborne Router. The purpose of this facility is to enable efficient management of the available subnetwork resources in areas of overlapping coverage. This facility is not appropriate when its use may result in an aircraft being denied air/ground data communications.

When a subnetwork connection is successfully established, then the procedures of 3.5.2.5 shall be applied to that subnetwork connection.

3.5.2.4 Air or Ground Initiated Route Initiation

Note 1.— Air or Ground-Initiated Route Initiation is only appropriate for Mobile Subnetworks that do provide connectivity information through a Join Event to both Airborne and Air/Ground Routers.

Note 2.— For Air or Ground-initiated subnetworks, the Join Event is received by the IS-SME in the Airborne or Air/Ground Router, respectively. The mechanism by which it is received is both subnetwork and implementation dependent.

On receipt of a Join Event, the Router shall either:

a) Issue an ISO 8208 Call Request with the DTE Address reported by the Join Event as the Called Address, or

b) Validate the DTE reported by the Join Event as to whether or not a subnetwork connection with it is acceptable according to local Routing Policy. If such a connection is acceptable then an ISO 8208 Call Request shall be issued with the DTE Address reported by the Join Event as the Called Address. Otherwise, the Join Event shall be ignored.

Note 3.— The Router validates the DTE that is the subject of the Join Event and determines the acceptability of a subnetwork connection with the so identified ATN Router, using procedures outside of the scope of this specification.

When a subnetwork connection is successfully established, then the procedures of 3.5.2.5 shall be applied to that subnetwork connection.

Note 4.— When a call collision occurs, then the call collision resolution procedures are applied by the SNDCF in order to ensure that only a single virtual circuit is established and that connection initiator and responder are unambiguously identified.

3.5.2.5 Exchange of Configuration Information using the ISO 9542 ISH PDU

ATN Airborne and Air/Ground Routers shall implement the ISO 9542 "Configuration Information" Function for use over each mobile subnetwork that they support. Whenever a subnetwork connection is established over a mobile subnetwork, the ISO 9542 Report Configuration Function shall be invoked in order to send an ISH PDU containing the NET of the Airborne or Air/Ground Router network entity over the subnetwork connection.

In the case of an Airborne Router, if it supports the use of IDRP for the exchange of routing information over this subnetwork, then the SEL field of the NET inserted into the ISH PDU shall always be set to 00h (a binary pattern of all zeroes). Alternatively, if the Airborne Router implements the procedures for the optional non-use of IDRP over this subnetwork then the SEL field of the NET inserted into the ISH PDU shall always be set to FEh (a binary pattern of 1111 1110).

Recommendation.— *When in the initiator role, an ATN Router should use the ISO 8208 "Fast Select" facility, if supported by the subnetwork, and encode the first ISH PDU in the Call Request user data, according to the procedures for the Mobile SNDCF specified in Chapter 7.*

Recommendation.— *When in the responder role and the initiator has proposed use of the Fast Select Facility, the ATN Router should encode the first ISH PDU in the Call Accept User Data, according to the procedures for the Mobile SNDCF specified in Chapter 7.*

Note 1.— The purpose of encoding an ISH PDU in call request/accept user data is to minimise the number of messages sent over limited bandwidth mobile subnetworks and the time taken to complete the route initiation procedures.

Whenever an ISO 9542 ISH PDU is received, either as Call Request/Accept user data, or as data sent over the connection, the Record Configuration function shall be invoked; the routing information necessary for NPDUs to be sent over the subnetwork connection to the indicated NET shall be written into the Forwarding Information Base for use by ISO 8473. A Systems Management Notification shall also be generated to report the arrival of the ISH PDU to the ATN Router's IS-SME.

3.5.2.6 Validation of the Received NET

The IS-SME shall, using the received NET to identify the remote ATN Router, validate the acceptability of a BIS-BIS connection with that remote ATN Router. If a BIS-BIS connection is unacceptable, then a Clear Request shall be generated to terminate the subnetwork connection. Forwarding Information associated with the subnetwork connection shall be removed from the Forwarding Information Base.

Note 2.— Except for the case of the situation described in 3.5.2.1.1, the acceptability of a BIS-BIS connection with the ATN Router identified by the received NET is determined using procedures outside of the scope of this specification.

If a BIS-BIS Connection is acceptable then an Air/Ground Router shall apply the procedures of 3.5.2.7, and an Airborne Router shall apply the procedures of 3.5.2.8.

3.5.2.7 Determination of The Routing Information Exchange Procedure by an Air/Ground Router

When the arrival of the ISH PDU is reported to the IS-SME of an Air/Ground Router, then the SEL field of the NET shall be inspected:

a) If the SEL field takes the value of 00h (a binary pattern of all zeroes), then this shall be taken to imply that the Airborne Router that sent this ISH PDU supports the use of IDRP for the exchange of routing information. The procedures of 3.5.2.9 shall be applied.

b) If the SEL field takes the value of FEh (a binary pattern of 1111 1110), then this shall be taken to imply that the Airborne Router that sent this ISH PDU supports the procedures for the optional non-use of IDRP for the exchange of routing information. The procedures of 3.5.2.11 shall be applied.

3.5.2.8 Determination of The Routing Information Exchange Procedure by an Airborne Router

When the arrival of the ISH PDU is reported to the IS-SME of an Airborne Router, then if the Airborne Router support the use of IDRP for the exchange of routing information, then the procedures of 3.5.2.9 shall be applied. If the Airborne Router supports the procedures for the optional non-use of IDRP for the exchange of routing information, then the procedures of 3.5.2.11 shall be applied.

3.5.2.9 Establishment of a BIS-BIS Connection

The IS-SME shall append the NET received on the ISH PDU to the **externalBISNeighbor** attribute of the BIS's **idrpConfig** Managed Object, if not already present, and create an **adjacentBIS** Managed Object for the remote ATN Router identified by this NET, if one does not already exist. An IDRP activate action shall then be invoked to start the BIS-BIS connection according to ISO/IEC 10747, if such a BIS-BIS connection does not already exist.

If the ISH PDU was received from a subnetwork connection which was established with the local ATN Router in the responder role, then the BIS-BIS connection shall be established with the **ListenForOpen** MO attribute set to false. Otherwise, the **ListenForOpen** MO attribute shall be set to true.

Note 1.— This procedure minimises the route initiation exchanges over a bandwidth limited mobile subnetwork. The reversal of initiator and responder roles for the BIS-BIS connection compared with the subnetwork connection ensures the fastest route initiation procedure.

If a BIS-BIS connection was already established with the remote ATN Router, then the IS-SME shall cause the IDRP Routing Decision function to be invoked in order to rebuild the FIB taking into account the additional subnetwork connectivity. This shall include re-update of the security information contained routes received from the remote ATN Router, according to Chapter 8.

The IS-SME shall also check to ensure that the procedures for the optional non-use of IDRP are not concurrently being applied to routing information exchange with an ATN Router with the same NET over a different subnetwork connection. This is an error and shall be reported to Systems Management; a BIS-BIS connection shall not be established in this case.

Recommendation.— *When IDRP is used to exchange routing information over an Air/Ground subnetwork, the value of the Holding Time field in the a BIS-BIS connection has been established, the periodic transmission of ISH PDUs should be set to 65534suppressed, except when a watchdog timer is applied to the subnetwork connection (see 3.5.2.12).*

Note 2.— The purpose of the above is to effectively suppress the generation of ISH PDUs.

Note 32.— Normally, the IDRP KeepAlive mechanism is sufficient to maintain a check on the "liveness" of the remote ATN Router. However, when watchdog timers are necessary it is also necessary to ensure a "liveness" check on a per subnetwork connection basis. The ISH PDU fulfils this role.

3.5.2.10 Exchange of Routing Information using IDRP

Once a BIS-BIS connection has been established with a remote ATN Router then:

a) An Airborne Router shall advertise routes to the Air/Ground Router in accordance with the Routing Policy specified in 3.7.2.

b) An Air/Ground Router shall advertise routes to the Airborne Router in accordance with the Routing Policy specified in 3.7.1.3 or 3.7.3.3 as appropriate for the role of the Air/Ground Router's RD.

3.5.2.11 Procedures for the Optional non-use of IDRP over an air-ground data link

Note.— In this case, there is no recommendation to suppress the periodic re-transmission of ISH PDUs according to the ISO 9542 Report Configuration Function. In the absence of IDRP, this re-transmission is necessary to maintain the "liveness" of the connection.

3.5.2.11.1 Air/Ground Router

Through the actions of the IS-SME as specified below, an Air/Ground Router shall simulate the existence of a BIS-BIS connection with an Airborne Router that implements the procedures for the optional non-use of IDRP by implementing the following procedure:

a) The NET of the remote ATN Router shall be appended to the **externalBISNeighbor** attribute of the BIS's **idrpConfig** Managed Object, if not already present, and an **adjacentBIS** Managed Object created for the

remote ATN Router identified by this NET, if one does not already exist. An Adj-RIB-in and an Adj-RIB-out shall hence be created for this remote ATN Router and for the Security RIB-Att.

Note 1.— No activate action will be applied to this MO and the implementation will hence need to be able to process information in the Adj-RIB-in even though the MO is in the "idle" state. There is also no need to ever place routes in the Adj-RIB-out. Implementations may choose to optimise the operation of these procedures with a special interface to IDRP.

b) Truncating the NET received on the ISH PDU to the first eleven octets and using the resulting NSAP Address Prefix as the NLRI of a route which is then inserted into the Adj-RIB-in for the remote ATN Router and identified by the Security RIB-Att, as if it had been received over a BIS-BIS connection. This route shall include an RD_Path attribute with the received NET as the Routing Domain Identifier of the originating RD, and an empty security path attribute.

Note 2.— According to the rules for the update of path information specified in Chapter 8, the security path attribute will be updated by the Routing Decision process to include an Air/Ground Subnetwork type security tag and an ATSC Class security tag, if this is appropriate. This procedure is identical to the normal use of IDRP over a mobile subnetwork.

The well-known mandatory path attribute RD_HOP_COUNT shall be set to 1 for routes to be inserted into the Adj-RIB-In of an A/G BIS for adjacent airborne BISs not implementing IDRP. In addition, for routes to be inserted into the Adj-RIB-In for adjacent airborne BISs not implementing IDRP, the well-known mandatory path attribute CAPACITY shall be set according to the capacity of the mobile subnetwork(s) over which the airborne BIS is reachable.

Note 3. — If the CAPACITY attribute is set to the value of the RD in which the Air/Ground BIS is located, the route pretends to provide the capacity of a ground subnetwork that is probably much higher than the capacity of the mobile subnetwork. This could result in inefficient forwarding decisions for NPDUs towards Airborne ESs. The CAPACITY attribute is correlated with the ATSC Class Security information.

If a subnetwork connection is concurrently established with the remote ATN Router over which the procedure for the optional non-use of IDRP have been applied, then the IS-SME shall not repeat the above procedures for the new subnetwork connection. Instead, the IS-SME shall cause the IDRP Routing Decision function to be invoked in order to rebuild the FIB taking into account the additional subnetwork connectivity. This shall include re-update of the security information contained routes received from the remote ATN Router, according to Chapter 8.

The IS-SME shall also check to ensure that a normal BIS-BIS connection does not concurrently exist with an ATN Router with the same NET. This is an error and shall be reported to Systems Management; the procedures for the optional non-use of IDRP shall not be applied in this case.

3.5.2.11.2 Airborne Router

An Airborne Router implementing the procedures for the optional non-use of IDRP over a mobile subnetwork shall simulate the operation of IDRP by maintaining a Loc-RIB for the Security RIB_Att, which is then used to generate FIB information.

Through the actions of its IS-SME, an Airborne Router shall derive entries for this loc_RIB from the ISH PDU received from an Air/Ground Router as follows:

a) The IS-SME shall insert into the loc-RIB, a route derived by truncating the NET received on the ISH PDU to the first eleven octets and using the resulting NSAP Address Prefix as the NLRI of a route. This route shall include a security path attribute with the Air/Ground Subnetwork Type and ATSC Class security tags (if any) determined from locally known information.

Note 1.— This provides routing information for destinations in the Air/Ground Router's RD and assumes that the eleven octet prefix of the Air/Ground Router's NET is common to all destinations in that RD.

b) The IS-SME shall insert into the loc-RIB, other routes available through the Air/Ground Router and determined using locally known information. This route shall include a security path attribute with the Air/Ground Subnetwork Type and ATSC Class security tags (if any) determined from locally known information.

Note 2.— As these routes are not subject to dynamic update, their availability must be ensured by the operator of the Air/Ground Router, within the limits specified for the applications that will use them.

3.5.2.12 Air-Ground Route Termination

Note 1.— The "Leave Event" is defined to signal when subnetwork connectivity with a remote ATN Router over a mobile subnetwork ceases to be available. This event may be generated by (a) the subnetwork itself using mechanisms outside of the scope of this specification, or (b) the SNDCF when it receives a clear indication from the subnetwork reporting either a network or a user initiated call clearing. The Leave Event is always reported to the IS-SME.

Note 2.— When a Leave Event is generated by a subnetwork, it applies to all subnetwork connections to a given DTE. When it is generated locally by the SNDCF, it typically applies to a single subnetwork connection.

Recommendation. — *A "Leave Event" should not be generated by the mobile SNDCF when a subnetwork connection is closed due to the expiration of the X.25 Idle timer, except if this subnetwork connection fails to be re-established.*

When a mobile subnetwork does not provide a network generated *Clear Indication* (e.g. to indicate that an aircraft has left the range of the mobile subnetwork, or when some other communication failure occurs, etc.), an ATN Router shall maintain a "watchdog" timer for each affected subnetwork connection and clear each such subnetwork connection once activity has ceased for a configurable period. When such a "watchdog" timer expires, this shall be reported as a "Leave Event" for that subnetwork connection.

Recommendation.— *The timer should be configurable according to the characteristics of the subnetwork.*

Note 3.— An ATN Router maintains a "watch-dog" timer for each applicable subnetwork connection to detect the event of an aircraft leaving coverage (or other communication failure), if such an event detection is not provided by the subnetwork.

When an IS-SME receives a Leave Event for a subnetwork connection or a DTE on a subnetwork, then it shall ensure that respectively, either the affected subnetwork connection or all subnetwork connections on that subnetwork and with the identified DTE, are cleared.

If, as a result of this procedure, there are no other subnetwork connections with the ATN Router that was the ultimate subject of the Leave Event then,

1. in the case of an ATN Router having established a BIS-BIS connection with that ATN Router, an IDRP deactivate action shall be invoked to terminate that BIS-BIS connection.~~except for the case of an Airborne Router implementing the procedures for the optional non-use of IDRP, an IDRP deactivate action shall be invoked to terminate the BIS-BIS connection with that ATN Router.~~

Note 4.— As a consequence of the deactivate action and following normal IDRP operation, the IDRP Routing Decision process will be invoked, the local FIB updated and routes previously available via the remote ATN Router may be withdrawn if suitable alternatives are not available.

2. In the case of an Air/Ground Router having simulated a BIS-BIS connection to an ATN Airborne Router, implementing the procedures for the optional non-use of IDRP, all routes shall be removed from the loc-RIB that had been inserted into it according to the procedures of section 3.5.2.11.1 as a result of an ISH PDU having been received from the Airborne Router for which the Leave Event reports a loss of connectivity.

3. In the case of an Airborne Router implementing the procedures for the optional non-use of IDRP, ~~the receipt of a Leave Event by the IS-SME shall result in the removal from the loc-RIB of~~ all routes shall be removed from the loc-RIB that had been inserted into it according to the procedures of section 3.5.2.11.2 as a result of an ISH PDU having been received from the Air/Ground Router for which the Leave Event reports a loss of connectivity.

If the BIS-BIS connection is not re-established within a period configurable from 1 minute to 300 minutes, or when the resources are required for other use, then the **adjacentBIS** Managed Object associated with the initiating BIS shall be deleted, and the initiating BIS's NET removed from the **externalBISNeighbor** attribute of the BIS's **idrpConfig** Managed Object.

3.5.2.13 APRL for Air/Ground Route Initiation

3.5.2.13.1 General

Item	Description	ATN SARPs Reference	CNS/ATM Package-1 Support
njSubnet	Support of Subnetworks that do not provide Join Event	3.5.2	O.1
jSubnet	Support of Subnetworks do provide a Join Event	3.5.2	O.1
giSubnet	Support of Ground Initiated Subnetworks	3.5.2	O.2
aiSubnet	Support of Air Initiated Subnetworks	3.5.2	O.2
agSubnet	Support of Air or Ground Initiated Subnetworks	3.5.2	O.2
fsSubnet	Support of Subnetworks that support Fast Select	-	O
~~noIDRP~~	~~Support of optional non-use of IDRP~~	~~3.5.2.11~~	~~O~~
noIDRP-a	Support of optional non-use of IDRP (Airborne BIS)	3.5.2.11.2	O
noIDRP-ag	Support of optional non-use of IDRP (Air/Ground BIS)	3.5.2.11.1	M
lvSubnet	Support of Subnetworks that provide a Leave Event	3.5.2.12	M

3.5.2.13.2 Airborne Router - Connection Responder

Item	Description	ATN SARPs Reference	CNS/ATM Package-1 Support
respAR-ar	Response to incoming Call Requests	3.5.2.1	giOragSubnet: M
valCR-ar	Validation of incoming Call Request	3.5.2.1	giOragSubnet:O
RespISH-ar	Generation of ISH PDU	3.5.2.5	giOragSubnet: M
ISHinCC-ar	Encoding ISH PDU in Connect Confirm User Data	3.5.2.5	RespISH-ar & fsSubnet: O
negNoIDRP-ar	Transmission of ISH with SEL field set to 0FEh	3.5.2.5	noIDRP-a:M
negIDRP-ar	Transmission of ISH with SEL field set to zero	3.5.2.5	^noIDRP-a:M
autoRoute-ar	Inference of available routes from A/G Router NET	3.5.2.11.2	noIDRP-a:M
initIDRP-ar	IDRP startup procedures - ListenForOpen set to false~~true~~	3.5.2.9	^noIDRP-a:M
supISH-ar	Suppression of multiple ISH PDUs	3.5.2.9	^noIDRP-a: O
valNET-ar	Validation of received NET	3.5.2.6	^noIDRP-a: O

giOragSubnet: giSubnet ^ agSubnet

3.5.2.13.3 Airborne Router - Connection Initiator

Item	Description	ATN SARPs Reference	CNS/ATM Package-1 Support

Item	Description	ATN SARPs Reference	CNS/ATM Package-1 Support
polling-ai	Procedures for polling a list of subnet addresses	3.5.2.2.1	pollReq: M
backoff-ai	Backoff Procedure	3.5.2.2.1.1	pollReq: M
connect-ai	Connect on receipt of Join Event	3.5.2.2.2	EventDrvn: M
ValJoin-ai	Validation of Join Event	3.5.2.2.2	EventDrvn: O
SendISH-ai	Generation of ISH PDU	3.5.2.5	EventDrvn ^ pollReq:M
ISHinCR-ai	Encoding of ISH PDU in Connect Request	3.5.2.5	SendISH-ar & fsSubnet: O
negNoIDRP-ai	Transmission of ISH with SEL field set to 0FEh	3.5.2.7	noIDRP-a:M
negIDRP-ai	Transmission of ISH with SEL field set to zero	3.5.2.7	^noIDRP-a:M
autoRoute-ai	Inference of available routes from A/G Router NET	3.5.2.11.2	noIDRP-a:M
initIDRP-ai	IDRP startup procedures - listenForOpen set to true~~false~~	3.5.2.9	^noIDRP-a:M
supISH-ai	Suppression of multiple ISH PDUs	3.5.2.9	^noIDRP-a: O
valNET-ai	Validation of received NET	3.5.2.6	^noIDRP-a: O

pollReq: aiSubnet & njSubnet

EventDrvn: jSubnet & (aiSubnet ^ agSubnet)

3.5.2.13.4 Air/Ground Router - Connection Responder

Item	Description	ATN SARPs Reference	CNS/ATM Package-1 Support
respAR-agr	Response to incoming Call Requests	3.5.2.1	aiOragSubnet: M
valCR-agr	Validation of incoming Call Request	3.5.2.1	aiOragSubnet:O
emgncy-agr	Emergency Procedures	3.5.2.1.1	M
RespISH-agr	Generation of ISH PDU	3.5.2.5	aiOragSubnet: M
ISHinCC-agr	Encoding ISH PDU in Connect Confirm User Data	3.5.2.5	RespISH-agr & fsSubnet: O
negNoIDRP-agr	Receipt of ISH with SEL field set to 0FEh	3.5.2.7	M
negIDRP-agr	Receipt of ISH with SEL field set to zero	3.5.2.7	M
autoRoute-agr	Inference of available routes from Airborne Router NET	3.5.2.11.1	M
initIDRP-agr	IDRP startup procedures - ListenForOpen set to false~~true~~	3.5.2.9	M
supISH-agr	Suppression of multiple ISH PDUs	3.5.2.9	^~~noIDRP:~~ O
valNET-agr	Validation of received NET	3.5.2.6	^~~noIDRP:~~ O

aiOragSubnet: aiSubnet ^ agSubnet

3.5.2.13.5 Air/Ground Router - Connection Initiator

Item	Description	ATN SARPs Reference	CNS/ATM Package-1 Support
connect-agi	Connect on receipt of Join Event	3.5.2.3	goOragSubnet: M
ValJoin-agi	Validation of Join Event	3.5.2.3	connect-agi: O
SendISH-agi	Generation of ISH PDU	3.5.2.5	connect-agi: M
ISHinCR-agi	Encoding of ISH PDU in Connect Request	3.5.2.5	Send-ISH-agi & fsSubnet: O
negNoIDRP-agi	Receipt of ISH with SEL field set to 0FEh	3.5.2.7	M
negIDRP-agi	Receipt of ISH with SEL field set to zero	3.5.2.7	M
autoRoute-agi	Inference of available routes from Airborne Router NET	3.5.2.11.1	~~noIDRP:~~M
initIDRP-agi	IDRP startup procedures - listenForOpen set to true~~false~~	3.5.2.9	^~~noIDRP:~~M
supISH-agi	Suppression of multiple ISH PDUs	3.5.2.9	^~~noIDRP:~~ O
valNET-agi	Validation of received NET	3.5.2.6	^~~noIDRP:~~ O

goOragSubnet: giSubnet ^ agSubnet

3.5.2.13.6 Termination Procedures

Item	Description	ATN SARPs Reference	CNS/ATM Package-1 Support
lvEvent	Processing of Leave Event	3.5.2.12	M
Watchdog	Watchdog Timer	3.5.2.12	M
ConfigWD	Configurability of Watchdog for Subnetwork Characteristics	3.5.2.12	O
conLeave	Processing of a per connection Leave Event	3.5.2.12	M
subnetLeave	Processing of a per Subnetwork Leave Event	3.5.2.12	M

3.6 Handling Routing Information

All ATN Routers in the same RD shall implement the same routing policy.

Note 1.— As specified in Chapter 8, an ATN Router supports both the empty (default) RIB_Att, and the RIB_Att comprising the Security Path Attribute identifying the ATN Security Registration Identifier~~, only~~. An ATN Router therefore includes two RIBs known as the default RIB and the Security RIB, each of which comprises a loc-RIB, and an Adj-RIB-in and an Adj-RIB-out for each adjacent BIS.

Note 2.— Each ATN RD will necessarily have a distinct routing policy that depends on its nature, and the nature of the RDs to which it is interconnected. This section specifies the baseline Routing Policy for each class of RD identified in

2.5. ATN RDs may then extend the specified baseline to match their actual requirements.

Note 3.— Each Routing Policy is expressed as a set of policy statements or rules.

Note 4.— These baseline policy statements given below are always subject to the ISO/IEC 10747 requirement that routes are only advertised when the DIST_LIST_INCL and DIST_LIST_EXCL path attributes, if present, permit the route to be so advertised. Routes may never be advertised to an RD or RDC which the route has already traversed.

3.7 Policy Based selection of Routes for Advertisement to Adjacent RDs

Note.— In general, the selection of routes for advertisement to adjacent Routing Domains is performed according to local routing policy rules. This specification mandates such routing policy rules for support of air-ground routing only. Routing Policy rules for support of ground-ground routing are a local matter.

3.7.1 Routing Policy Requirements for Members of an ATN Island Backbone RDC

An ATN RD that is a member of an ATN Island Backbone RDC shall implement a Routing Policy that is compatible with the policy statements given in this section and its subordinate sections.

Note.— The routing policies expressed in this section do not constrain RD policies as much as define whether an RD's policies define it as being in the backbone or not.

3.7.1.1 Adjacent ATN RDs within the Backbone RDC

Note 1.— These policy statements apply to the routes advertised by an ATN Router in a RD that is a member of a Backbone RDC, to an adjacent ATN Router in a different RD, which is also a member of the same ATN Island Backbone RDC.

Each ATN Router that is in an RD that is a member of an ATN Island's Backbone RDC, shall provide the following routes to each adjacent ATN RD within the same Backbone RDC, and for the Security RIB-Att :

a) A route to NSAPs and NETs contained within the RD; the route's destination shall be one or more NSAP Address prefixes common to all NSAP Addresses and NETs in the RD. If restrictions on distribution scope are applied by local routing policy, then they shall not prevent distribution of this route to any member of the same ATN Island backbone RDC.

   Note 2.— The well known discretionary attribute DIST_LIST_INCL may also be present. For example, to restrict the scope of the information to members of the ATN Backbone RDC only. The RDIs of other RDs and RDCs may also be present at the discretion of the local Administrative Domain, and by bilateral agreement.

   Note 3.— The objective of this rule is to ensure that a member of a backbone RDC will tell all its neighbours within the backbone about itself.

b) The selected route to every Mobile RD for which a route is available.

   Note 4.— The objective of this rule is to ensure that a member of a backbone RDC will inform all other backbone RDC members within the island about all routes to all mobiles that it has available.

c) The selected route to every Fixed ATN RD in the same ATN Island, for which a route is available.

   Note 5.— The objective of this rule is to ensure that a member of a backbone RDC will tell other members of the same backbone RDC about all fixed RDs that it knows about.

d) Each selected route to a Mobile RD's "home".

   Note 6.— The objective of this rule is to ensure that a member of a backbone RDC will tell all fixed RDs about all the "homes" that it knows about.

   Note 7.— Such a route can be characterised by an NSAP Address Prefix which ends at the VER field and the VER field takes either the value 041h or the value 0c1h.

3.7.1.2 All other ATN RDs within the ATN Island

Note 1.— These policy statements apply to the routes advertised by an ATN Router in an RD that is a member of a Backbone RDC to an adjacent ATN Router in a different RD, which is also a member of the same ATN Island RDC, but which is not a member of that ATN Island's Backbone RDC.

An ATN Router that is in an RD that is a member of an ATN Island Backbone RDC shall provide the following routes to each adjacent ATN RD within the ATN Island RDC, which are not members of the ATN Island's Backbone RDC, and for the Security RIB-Att :

a) A route to NSAPs and NETs contained within the RD; the route's destination shall be one or more NSAP Address prefixes common to all NSAP Addresses and NETs in the RD. If restrictions on distribution scope are applied by local routing policy, then they shall not prevent distribution of this route to any member of the same ATN Island RDC.

Note 2.— The well known discretionary attribute DIST_LIST_INCL may also be present. For example, to restrict the scope of the information to members of the ATN Island only. The RDIs of other RDs and RDCs may also be present at the discretion of the local Administrative Domain, and by bilateral agreement.

Note 3.— The objective of this rule is to ensure that a member of a backbone RDC will tell all RDs within the island about itself.

b) The selected route to every Fixed ATN RD in the same ATN Island for which a route is available.

Note 4.— The objective of this rule is to ensure that an ATN Router located in an RD that is a member of a backbone RDC, will tell all RDs within the island about all the fixed RDs it knows about.

c) A route to all AINSC mobiles and all ATSC Mobiles. The well known discretionary attribute DIST_LIST_INCL shall be present, and shall contain the RDI of the ATN Island RDC as its value. The Security Path attribute shall contain an ATSC Class Security Tag indicating support for all ATSC Classes supported for Air/Ground data interchange, if any.

Note 5.— The objective of this rule is to tell the rest of the Island that each RD in the Backbone RDC provides a default route to all aircraft.

Note 6.— The distribution scope of the route is limited because the ATN Island defines the domain of the default route provider. This route is invalid outside of the ATN Island.

Note 7.— This route is formally the result of aggregating all the routes to mobile systems and routes to "Home" RDs, known to the ATN Router.

d) A route to each Mobile RD for which the adjacent RD is advertising a route to the Mobile RD's "home".

Note 8.— The objective of this rule is to ensure that a member of a backbone RDC will tell all adjacent off Backbone RDs about all routes to mobile RDs which have "home" routes advertised.

3.7.1.3 Mobile RDs

Note 1.— These policy statements apply to the routes advertised by an ATN Router in an RD that is a member of a Backbone RDC to an adjacent ATN Router in a Mobile RD.

When IDRP is being used to exchange routing information with an airborne router, an ATN Router in an RD that is a member of a Backbone RDC shall provide to each adjacent Mobile RD a route to NSAPs and NETs contained within the RD for the Security RIB-Att; the route's destination shall be one or more NSAP Address prefixes common to all NSAP Addresses and NETs in the RD.

Note 2.— The objective of this rule is to ensure that an RD that is a member of a backbone RDC will tell all adjacent mobiles about itself.

Recommendation.— *An ATN RD that is a member of a Backbone RDC should also provide to each adjacent Mobile RD, and for the Security RIB-Att and for which a suitable route exists:*

a) *An aggregated route to NSAPs and NETs contained within the local ATN Island RDC;*

Note 3.— The objective of this rule is to ensure that an RD that is a member of a backbone RDC provides to each connected mobile RD, a route to all fixed ATN RDs within the island.

b) *An aggregated route to NSAPs and NETs contained within all other ATN Islands for which a route is available.*

Note 4.— The objective of this rule is to ensure that an RD that is a member of a backbone RDC will be willing to provide to each connected mobile RD routing information to the backbone of other ATN islands.

3.7.1.4 ATN RDs in other ATN Islands

Note 1.— These policy statements apply to the routes advertised by an ATN Router in an RD that is a member of a Backbone RDC to an adjacent ATN Router in a different RD, which is a member of a different ATN Island's ATN Island Backbone RDC.

An ATN Router in an RD that is a member of a Backbone RDC shall provide the following routes to each adjacent ATN Router that is a member of a Backbone RDC in another ATN Island, and for the Security RIB-Att :

a) An aggregated route to NSAPs and NETs contained within the ATN Island RDC.

Note 2.— The objective of this rule is to ensure that an RD that is a member of a backbone RDC will tell all adjacent RDs that are members of backbone RDCs in different ATN Islands about the local ATN Island.

b) A route to the common NSAP Address Prefix for each group of Mobile RDs for which the "home" exists on the RD's ATN Island.

Note 3.— The objective of this rule is to ensure that a backbone RD will tell all adjacent RDs that are member of a backbone RD in different islands about routes to mobiles whose "home" is in that island.

Note 4.— The "home" identified above needs not correspond to a geographical notion of a home.

Note 5.— The "home" is typically identified by an NSAP Address Prefix that identifies all the RD's belonging to the organisation responsible for the Mobile RD (i.e. aircraft), or all the Mobile RDs belonging to the organisation. The former is only possible if all such Fixed RDs are part of the same ATN Island RDC.

c) A route to each Mobile RD for which the adjacent RD is advertising a route to the Mobile RD's "home".

Note 6.— The objective of this rule is to ensure that a member of a backbone RDC will tell all adjacent RDs in different islands about all routes to mobile RDs which have "home" routes advertised.

d) A route to each Mobile RD for which there is no known home.

Note 7.— The objective of this rule is to ensure that an RD that is a member of a backbone RDC will tell all adjacent RDs that are members of backbone RDCs in different ATN Islands about all of the Mobile RDs that they know about.

3.7.2 Routing Policy Requirements for a Mobile RD

When IDRP is being used to exchange routing information with an airborne router, a Mobile RD shall provide to each ATN RD to which it is currently connected, a route to NSAPs and NETs contained within the Mobile RD for the Security RIB-Att .

Note 1.— The objective of this rule is to ensure that a mobile RD will tell adjacent RDs about itself.

Note 2.— This policy statement applies to the routes advertised by an ATN Router in a Mobile RD to an adjacent ATN Air/Ground Router in a Fixed ATN RD.

3.7.3 Routing Policy Requirements for an ATN TRD that is not a Member of the ATN Island Backbone RDC

An RD that is a member of an ATN Island RDC, and is a TRD, but which is not a member of that ATN Island's Backbone RDC shall implement a Routing Policy that is compatible with the policy statements given in this section and its subordinate sections.

Note.— An ATN RD that operates as a transit routing domain is referred to in this chapter as an ATN TRD.

3.7.3.1 Adjacent ATN RDs that are Members of the ATN Island's Backbone RDC

Note 1.— These policy statements apply to the routes advertised by an ATN Router in an ATN TRD to an adjacent ATN Router in an RD which is a member of the local ATN Island's Backbone RDC.

When an ATN TRD that is not itself a member of a Backbone RDC is adjacent to an RD that is a member of an ATN Backbone RDC, then it shall provide the following routes to each such adjacent ATN RD, and for the Security RIB-Att :

a) A route to NSAPs and NETs contained within the RD; the route's destination shall be one or more NSAP Address prefixes common to all NSAP Addresses and NETs in the RD.

Note 2.— The well known discretionary attribute DIST_LIST_INCL may also be present. For example, to restrict the scope of the information to members of the ATN Island only. The RDIs of other RDs and RDCs may also be present at the discretion of the local Administrative Domain, and by bilateral agreement.

Note 3.— The objective of this rule is to ensure that an ATN TRD that is not itself a member of the Backbone RDC, will tell all adjacent ATN RDs which are members of the Backbone RDC about itself.

b) The selected route to every Mobile RD for which a route is available.

Note 4.— The objective of this rule is to ensure that a ATN TRD that is not itself a

member of the Backbone RDC, will tell all adjacent ATN RDs which are members of the Backbone RDC about all mobiles it knows about.

c) The selected route to every Fixed ATN RD in the ATN Island for which a route is available.

Note 5.— The objective of this rule is to ensure that a ATN TRD that is not itself a member of the Backbone RDC, will tell all adjacent ATN RDs which are members of the Backbone RDC about all fixed RDs it knows about in the same ATN Island.

d) A route to each "Home" that the ATN TRD itself provides for Mobile RDs. This route has as its destination, the common NSAP Address Prefix(es) for those Mobile Rds. The Security Path attribute shall contain an ATSC Class Security Tag indicating support for all ATSC Classes supported for Air/Ground data interchange, if any.

Note 6.— The objective of this rule is to support the operation of the Home Domain concept on any ATN TRD directly connected to a Backbone RD.

3.7.3.2 Adjacent ATN RDs within the same ATN Island and which are not Members of the ATN Island's Backbone RDC

Note 1.— These policy statements apply to the routes advertised by an ATN Router in an ATN TRD to an adjacent ATN Router in an ATN RD on the same ATN Island.

An ATN TRD shall provide the following routes to each adjacent ATN RD within the ATN Island RDC, other than other ATN RDs which are members of the Backbone RDC, and for the Security RIB-Att

a) A route to NSAPs and NETs contained within the RD for the Security RIB-Att; the route's destination shall be one or more NSAP Address prefixes common to all NSAP Addresses and NETs in the RD.

Note 2.— The well known discretionary attribute DIST_LIST_INCL may also be present. For example, to restrict the scope of the information to members of the ATN Island only. The RDIs of other RDs and RDCs may also be present at the discretion of the local Administrative Domain, and by bilateral agreement, including the RDI of the Backbone RD or RDC, when the adjacent RD is providing the local RD's route to the Backbone.

Note 3.— The objective of this rule is to ensure that an ATN TRD that is not itself a member of the Backbone RDC, will tell all adjacent RDs within the island about itself.

b) The selected route to every Fixed RD in the same ATN Island for which a route is available.

Note 3.— The objective of this rule is to ensure that an ATN TRD that is not itself a member of the Backbone RDC, will tell all adjacent RDs within the island about all fixed ATN RDs in the same ATN Island that it knows about.

c) If the RD is currently advertising the preferred route to all AINSC and ATSC Mobiles, then every route to an AINSC Mobile and an ATSC Mobile that is known to the local RD shall be advertised to this RD, subject only to constraints imposed by any DIST_LIST_INCL and DIST_LIST_EXCL path attributes.

Note 4 .— The objective of this rule is to ensure that the provider of the default route to all aircraft (i.e. the Backbone) is kept informed of the actual location of every aircraft adjacent to the Island.

d) The preferred route to all mobiles, except when the RD is the source of this route.

Note 5.— The objective of this rule is to ensure propagation of the default route to all mobiles throughout the ATN Island.

e) A route to each Mobile RD for which the adjacent RD is advertising the preferred route to the Mobile RD's "home".

Note 6.— The objective of this rule is to ensure routes to mobile RDs are propagated to off backbone Homes.

f) A route to each "Home" that the ATN TRD itself provides for Mobile RDs. This route has as its destination, the common NSAP Address Prefix(es) for those Mobile Rds. The Security Path attribute shall contain an ATSC Class Security Tag indicating support for all ATSC Classes supported for Air/Ground data interchange, if any.

Note 7.— The objective of this item is to ensure that all RDs in the ATN Island are aware that the identified "Homes" are located here.

3.7.3.3 Mobile RDs

Note 1.— These policy statements apply to the routes advertised by an ATN Router in an ATN TRD to an adjacent ATN Router in a Mobile RD.

When IDRP is being used to exchange routing information with the airborne router, an ATN

TRD shall provide to each adjacent Mobile RD a route to NSAPs and NETs contained within the RD for the Security RIB-Att ; the route's destination shall be one or more NSAP Address prefixes common to all NSAP Addresses and NETs in the RD.

Note 2.— The objective of this rule is to ensure that an ATN TRD will tell adjacent mobile RDs about itself.

Recommendation.— *An ATN TRD should also provide to each adjacent Mobile RD, and for the Security RIB-Att and for which a suitable route exists:*

a) an aggregated route to NSAPs and NETs contained within the local ATN Island RDC;

b) *an aggregated route to NSAPs and NETs contained within all other ATN Islands for which a route is available.*

Note 3.— The objective of this rule is to encourage an RD to provide to each adjacent mobile RD routing information to: a) all fixed RDs within the island, and b) other ATN islands.

3.7.4 The Routing Policy for a Fixed ATN ERD

A Fixed ATN ERD shall provide to each ATN RD to which it is currently connected, a route to NSAPs and NETs contained within the RD, for the Security RIB-Att .

Note 1.— The well known discretionary attribute DIST_LIST_INCL may be present, unless the RD permits routes to destinations within itself to be advertised by other ATN RDs without restriction to any other ATN RD, or non-ATN RD.

Note 2.— These policy statements apply to the routes advertised by an ATN Router in a fixed ATN ERD to an adjacent ATN Router in an ATN RD.

Note 3.— An ERD does not advertise routes to destinations in any other RD, to another RD.

3.8 Use of the Forwarding Information Base

The forwarding processes for a CLNP NDPU shall operate by selecting the FIB identified by the combination of the QoS Maintenance and Security Parameters found in the CLNP Header, and selecting from that FIB, the entry, if any, identified by the longest matching NSAP Address Prefix. The next hop information found in this FIB entry is then used to forward the NPDU.

~~Two routes shall only be aggregated when their SECURITY attributes, if present, identify the same Security Policy. When two routes are aggregated, if a security classification is present in either of the component routes, then the classification of the aggregated route shall be set to the lower of the two classifications.~~

4. NETWORK AND TRANSPORT ADDRESSING SPECIFICATION

4.1 General Provisions

Note 1.— The ATN internetwork addressing plan defines an OSI Network Service Access Point (NSAP) address structure which can support efficient internetwork routing procedures, and which conforms to common abstract syntax, semantic and encoding rules throughout the ATN OSI environment.

Note 2. — In general, where reference is made in this chapter to delegation of administrative responsibility by ICAO to States or organisations, it is expected that the practical effect of this delegation is that the respective States or organisations assume full administrative duties related to the delegated responsibilities. This means, for example, that if ICAO delegates to one or more States or organisations the responsibility for allocation, assignment and general administration of particular segments of the ATN address space, then those States or organisations must place into operation the necessary administrative structure to carry out the delegated allocation, assignment and administration activities. After having carried out the delegated administration of these field values, the State or organisation is then obliged to inform ICAO on a mutually agreed basis of administrative actions taken, so that ICAO may fulfill its responsibility as the ATN addressing authority in terms of publication and communication of this information for use by the civil aviation community. It is also important to note that a State or organisation may request delegation by ICAO of direct responsibility for its own administrative address space, if and when that State or organisation wishes to commence its own administrative activities. Finally, it is important to note that the role of ICAO in this area is one of international coordination, advice and consultation in order to ensure orderly and efficient operation of the global aspects of the ATN. Thus, ICAO may be expected to provide counsel to States and organisations having assumed such delegated responsibilities, in order to ensure that address administration is carried out in a manner that supports the orderly and efficient global operation of the ATN internet

4.1.1 Addressing Plan Scope

The *Aeronautical Telecommunication Network* (ATN) OSI *Network Service Access Point* (NSAP) Addressing Plan shall be used by OSI end-systems and intermediate-systems participating in the aeronautical OSIE.

Note.— The ATN NSAP Addressing Plan serves the needs of a variety of aeronautical data communication user groups, including Air Traffic Service Communications (ATSC) and Aeronautical Industry Services Communications (AINSC) users.

4.1.2 Addressing Plan Applicability

The ATN NSAP Addressing Plan shall be applicable to the identification of both fixed and mobile end-systems and intermediate-systems.

Note.— The ATN NSAP Addressing Plan defines the Network Layer addressing information to be utilized by ATN end-systems, and by ATN intermediate-systems.

4.1.3 Addressing Goal

ATN NSAP addresses shall provide unambiguous identification of NSAPs and network entities located in OSI end-systems and intermediate-systems operating within the ATN OSI environment.

Note. — In meeting this goal, it is important to consider the impact of address assignment strategies on the quantity and frequency of exchange of routing information. In other words, while it is a given that the unambiguous identification of Network entities is the primary goal of the assignment of Network addresses, it is also true that without due caution, both routing information exchange efficiency and the resulting effectiveness of routing aggregation may be adversely affected. These effects must be considered when performing the administrative functions of address assignment and field value allocation.

4.1.4 Conformance to ISO Standards

ATN NSAP addresses shall conform to ISO 8348.

4.1.5 ISO Address Format Definition

ATN NSAP addresses shall employ an International Code Designator (ICD) format Domain Specific Part (DSP) using binary DSP syntax.

4.1.6 Subnetwork Independence

The ATN NSAP Addressing Plan shall not depend upon particular subnetwork address syntax, semantics or encoding techniques.

Note.— This facilitates the internetworking of End Systems and Intermediate Systems operated by various end-users and service providers within the aeronautical domain, while allowing these end-users and service providers to retain local control of local end-system and subnetwork operations.

4.1.7 Address Mapping

Routing and forwarding functions within ATN End-Systems and Intermediate-Systems shall perform any required mapping of ATN NSAP address formats to SNPA address formats required on interconnecting data subnetworks.

Note.— For this reason, only ATN Host Computers (i.e. end systems) and Routers (i.e. intermediate systems) need evaluate the contents of an ATN NSAP address.

4.1.8 Address Transfer

ATN NSAP address information shall be transferred transparently between adjoining ATN Network Layer entities, by means of interconnecting data subnetworks. Valid ATN NSAP address syntaxes must transit unchanged via data encoding or data compression techniques employed in association with these interconnecting data subnetworks.

Note.— ATN NSAP address formats may be carried over any aeronautical subnetwork which provides bit-oriented (i.e. transparent) transfer of subnetwork user data fields, including those fields carrying Network Layer protocol headers.

4.1.9 Definition of a Network Entity Title

Note 1.— A Network Entity Title (NET) is the unique name of a Network Entity (NE) contained in an End system (ES) or in an Intermediate System (IS). It is used to unambiguously identify a given NE. An End- or Intermediate System may comprise multiple NE's, in which case each will be identified by a unique NET.

Note 2.— NET's are assigned from the same addressing space as Network Service Access Point (NSAP) addresses. The authority which is responsible for allocating addresses from a given address space to NSAP's, may choose also to allocate NET's following the same procedures and rules it observes in the allocation of NSAP's.

Note 3.— NET's and NSAP addresses are syntactically indistinguishable; any value that the responsible authority is permitted to allocate as an NSAP address may be allocated as a NET.

Note 4.— The ATN NSAP Addressing Plan mandates specific values for the Selector (SEL) field for two types of NE's contained in ATN Intermediate Systems, as given in section 4.5.9.3

4.1.10 Addressing Administrative Domains

ATN end-systems or intermediate-systems located on-board general aviation aircraft shall belong to an ATSC administrative domain, whereas ATN systems located on-board commercial aircraft shall belong to an AINSC administrative domain.

4.2 Administrative Provisions

Note.— This clause specifies general provisions applicable to the administration of the ATN internetwork addressing plan.

4.2.1 Syntax Administration

The ATN NSAP address syntax (i.e. field boundaries, sizes and formats) shall be defined and administered by ICAO as the international aeronautical authority.

4.2.2 Semantic Administration

The ATN NSAP address semantics (i.e. field content and interpretation) shall be defined and administered by ICAO as the international aeronautical authority.

Note.— Authority for the semantic content of particular fields may be delegated by ICAO to other State, aeronautical and telecommunication standards authorities.

4.2.3 Encoding Administration

The ATN NSAP address encoding procedures (i.e. the representation of abstract syntax and semantics in machine-readable form) shall be administered by ICAO as the international aeronautical authority.

Note.— Authority for the encoding of particular fields may be delegated by ICAO to other State,

aeronautical and telecommunication standards authorities.

4.3 Abstract Syntax Provisions

The Domain Specific Part (DSP) of the ATN NSAP Addresses shall be represented in the binary abstract syntax.

Note 1.— The Initial Domain Part (IDP) is specified in ISO 8348 to have a decimal abstract syntax.

Note 2.— For the purpose of administration and assignment of ATN NSAP Addresses, the NSAP address format includes nine fields, two of which comprise the IDP (AFI and IDI) and the remaining seven of which comprise the DSP. The AFI and IDI follow the ISO standard and thus have a decimal abstract syntax. However, certain DSP fields are derived from existing ICAO and IATA registration schemes and are not specified in a native binary form. Rules for the translation of their native abstract syntaxes to the required binary abstract syntax are provided in this specification.

4.3.1 Format Definition

The ATN NSAP address format shall comprise nine (9) fields, as specified in Figure 4-1.

4.3.2 Field Abstract Syntax

The address field abstract syntax shall be as specified in Table 4-1.

4.3.3 Field Syntax Construction

All fields shall be right-justified, and shall be filled with leading ‘‘**0**” digits (for decimal or hexadecimal syntax fields) or leading ‘‘**@**” characters (for alphanumeric syntax fields) as required to produce fields of specified fixed lengths.

4.3.4 Reserved Values in Address Fields

Address field values specified as "reserved" shall not be used until assigned by ICAO.

Note.— These field values are currently unassigned, and are retained by ICAO for future assignment.

4.3.5 Unassigned Values in Address Fields

Address field values specified as "spare" shall be available for local use until assigned by ICAO.

Note.— These field values are currently unassigned, and are retained by ICAO for future assignment.

4.4 Encoding Provisions

Note.— This clause specifies general provisions applicable to the encoding rules of the ATN internetwork addressing plan.

4.4.1 Field Encoding Definition

The address field encoding shall be as specified in Table 4-1.

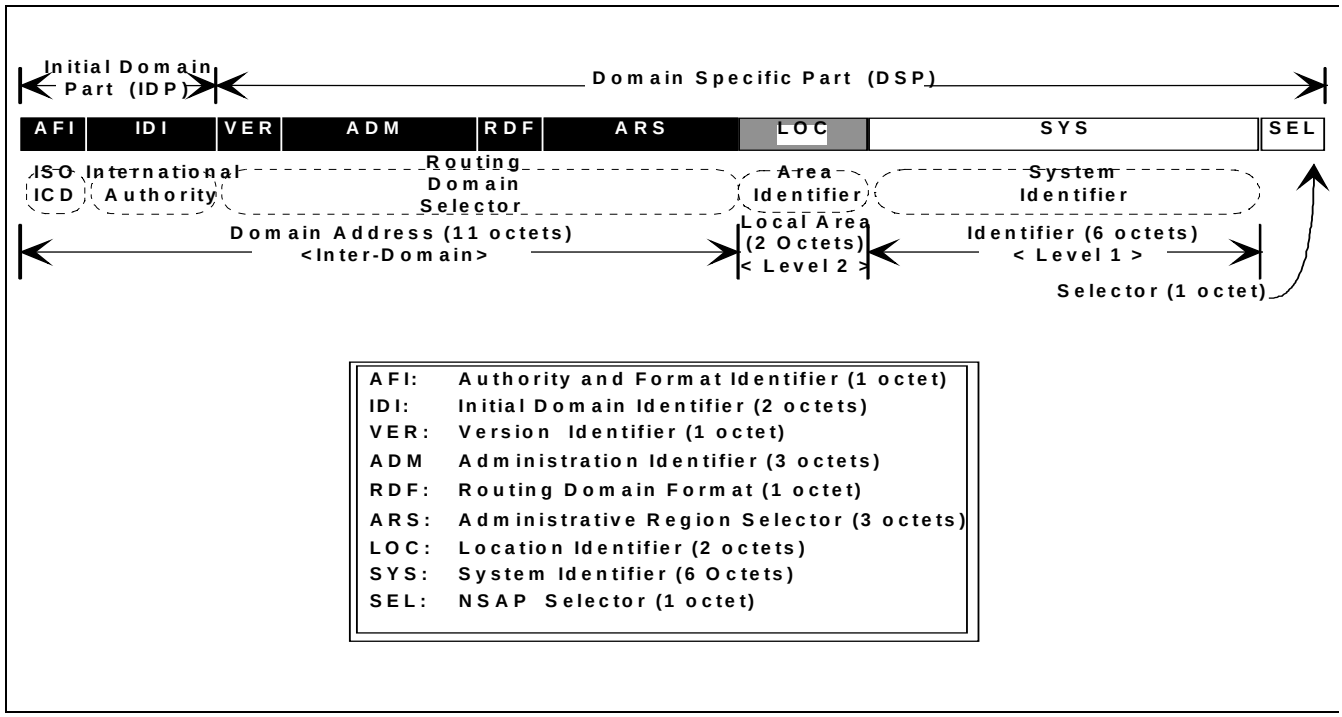


Figure 4-1: ATN NSAP Address Format

Address Field Name	Address Field Size	Field Abstract Syntax	Digit/Character Count	Field Encoding
VER	1 Octet	Hexadecimal	2 Digits	Binary
ADM	3 Octets	Hexadecimal	6 Digits	Binary
RDF	1 Octet	Hexadecimal	2 Digits	Binary
ARS	3 Octets	Hexadecimal	6 Digits	Binary
SYS	6 Octets	Hexadecimal	12 Digits	Binary

Table 4-1: ATN NSAP Address Field Characteristics

4.4.2 Fill Bits

Unspecified leading bits in all encoded fields shall be filled with the binary value ‘‘**0**”.

4.4.3 Field Size

All encoded fields shall be fixed in size, as specified in Table 4-1.

4.4.4 Encoding of Decimal Syntax

The BCD numeric digit set shall comprise the ten digits ‘‘**0**” through ‘‘**9**”. BCD field digits shall be represented with 4-bit binary numbers ranging in encoded decimal values from **[0]** through **[9]**.

4.4.5 Encoding of Hexadecimal Syntax

The hexadecimal digit set shall comprise the sixteen digits ‘‘**0**” through ‘‘**9**”, and ‘‘**a**” through ‘‘**f**”. Hexadecimal field digits shall be represented with 4-bit binary numbers ranging in encoded decimal values from **[0]** through **[15]**.

4.4.6 Encoding of Alphanumeric Syntax

The alphanumeric character set shall comprise the International Alphabet No. 5 (IA-5) character set, and shall be encoded according to IA-5 encoding rules.

4.4.7 Encoding of Identifier Syntax

The identifier meta-character set shall comprise the list of all three-character identifiers composed from the character set including only:

- the decimal numerals ‘‘**0**” through ‘‘**9**”, with decimal ordinal values **[0]** through **[9]**;
- the symbol ‘‘**@**”, with decimal ordinal value **[10]**; and,
- the upper-case alphabet ‘‘**A**” through ‘‘**Z**”, with decimal ordinal values **[11]** through **[37]**.

The resulting list of identifier metacharacters shall comprise a range in abstract syntax from ‘‘**000**” through ‘‘**ZZZ**”, with an ordinal range in encoded decimal values from **[0]** through **[50652]**.

Note 1.— This construct may be viewed as a three-digit radix-37 number.

Note 2.— This encoding mechanism is provided to support the optional mapping of certain IATA-defined character-based identifiers into binary address fields.

4.5 Address Field Provisions

Note.— This clause specifies the detailed requirements for each of the nine fields which form the ATN NSAP address.

Note.— Field value specifications are enclosed in square brackets (i.e. [ ]*), with syntax as noted (i.e. hexadecimal, decimal, alphanumeric or identifier).*

4.5.1 Authority/Format Identifier

Note.— The Authority/Format Identifier (AFI) field specifies the authority responsible for allocating values for the IDI field, the format of the IDI field, and the abstract syntax

representation used for the Domain Specific Part (DSP) of the NSAP address.

4.5.1.1 Format

The AFI field shall contain the two-digit decimal representation of the ATN NSAP Authority and Format Identifier.

4.5.1.2 Administration

Note.— The AFI field value for an ATN NSAP address has been selected by ICAO from the set of values specified by ISO.

4.5.1.3 Range

The AFI field value for an ATN NSAP address shall be **[47]**, expressed as a decimal number.

4.5.1.4 Encoding

The AFI field shall be encoded using BCD rules, as defined in 4.4.4.

4.5.2 Initial Domain Identifier

The Initial Domain Identifier (IDI) field shall specify the abstract syntax and semantics of the DSP portion of the ATN NSAP address.

4.5.2.1 Format

The IDI field shall contain the four-digit decimal representation of the International Code Designator which defines an ICAO-administered ATN NSAP DSP format.

4.5.2.2 Administration

Note.— The IDI value is registered with ISO as defined in ISO 6523.

4.5.2.3 Range

The IDI field value for an ATN NSAP address shall be **[0027]**, expressed as a decimal number.

4.5.2.4 Encoding

The IDI field shall.be encoded using BCD rules, as defined in 4.4.4.

4.5.3 Version Identifier

The Version Identifier (VER) field shall specify the version number applicable to the ATN NSAP address syntax, semantics and encoding.

4.5.3.1 Format

The VER field shall contain the two-digit hexadecimal representation of the version number for the ATN NSAP Address.

4.5.3.2 Administration

Note.— The VER field value for an ATN NSAP address is defined by ICAO.

4.5.3.3 Range

The VER field value for Version 1 of the AINSC ATN NSAP Address in fixed systems, expressed as a two-digit hexadecimal number, shall be **[01]**.

The VER field value for Version 1 of the AINSC ATN NSAP Address in mobile systems, expressed as a two-digit hexadecimal number, shall be **[41]**.

The VER field value for Version 1 of the ATSC ATN NSAP Address in fixed systems, expressed as a two-digit hexadecimal number, shall be **[81]**.

The VER field value for Version 1 of the ATSC ATN NSAP Address in mobile systems, expressed as a two-digit hexadecimal number, shall be **[c1]**.

Future versions of the AINSC ATN NSAP Address shall be allocated VER field values in the range **[02] - [3f]** for fixed systems and **[42] - [7f]** for mobile systems; these values shall be reserved until they are assigned. Future versions of the ATSC ATN NSAP Address shall be allocated VER field values in the range **[82] - [bf**] for fixed systems and **[c2] - [ff]** for mobile systems; these values shall be reserved until they are assigned. The VER field values **[00], [40], [80]** and **[c0]** shall be reserved.

4.5.3.4 Encoding

The VER field shall be encoded using binary rules, as defined in 4.4.5.

4.5.4 Administration Identifier

The Administration Identifier (ADM) field shall specify the organization responsible for administration of an ATN Administrative Domain.

4.5.4.1 Format

The format of the ADM field shall be as given in 4.5.4.1.1 or 4.5.4.1.2, based on whether the organization responsible for administration of the associated ATN Administrative Domain is an ATSC organization or an AINSC organization.

4.5.4.1.1 ATSC Format

The ATSC ADM field shall contain the six-digit hexadecimal code for an ATSC Administrative Domain identifier.

This field value shall be derived from the set of three-character alphanumeric symbols representing a three-character ISO country designator as defined in ISO 3166.

4.5.4.1.2 AINSC Format

The AINSC ADM field shall contain the six-digit hexadecimal code for an AINSC Administrative Domain identifier.

Recommendation.— *This field value should be derived from the set of three-character alphanumeric symbols representing an IATA Airline or Aeronautical Stakeholder Designator.*

4.5.4.2 Administration

ADM field values shall be administered by the authority given in 4.5.4.2.1 or 4.5.4.2.2, based on whether the associated ATN Administrative Domain is an ATSC domain or an AINSC domain.

4.5.4.2.1 ATSC Administration

ATSC ADM values shall be assigned and administered by ICAO.

Note.— Authority may be further delegated to State authorities as required.

4.5.4.2.2 AINSC Administration

AINSC ADM values shall be assigned and administered by IATA.

Note.— Authority may be further delegated to aeronautical industry authorities as required.

4.5.4.3 Range

The range of ADM field values shall be determined as given in 4.5.4.3.1 or 4.5.4.3.2, based on whether the associated ATN Administrative Domain is an ATSC domain or an AINSC domain.

4.5.4.3.1 ATSC Range

The ATSC ADM field values shall be in the range **[000000]** - **[ffffff]**, represented as hexadecimal numbers.

The ATSC ADM field shall contain the IA-5 encoding of valid three-character alphanumeric ISO Country Code values, as specified in ISO 3166. For this purpose, the ATSC ADM field shall be represented using upper-case alphabetic characters and decimal numerals.

4.5.4.3.2 AINSC Range

The AINSC ADM field values shall be in the range **[000000]** - **[ffffff]**, represented as hexadecimal numbers.

Recommendation.— *The AINSC ADM field should contain the IA-5 encoding of valid three-character alphanumeric IATA Airline or Aeronautical Stakeholder Designator values, as specified in the IATA Airline Coding Directory. For this purpose, the AINSC ADM field should be represented using upper-case alphabetic characters and decimal numerals.*

4.5.4.4 Encoding

The ADM field shall be encoded using alphanumeric rules, as defined in 4.4.6.

4.5.5 Routing Domain Format

The Routing Domain Format (RDF) field shall be reserved.

The RDF field value shall be **[00]** expressed as a two-digit hexadecimal number.

The RDF field shall be encoded using binary rules, as defined in 4.4.5.

4.5.6 Administrative Region Selector

The Administrative Region Selector (ARS) field shall identify the routing domain of the addressed network entity.

Note 1.— In the case of a fixed (i.e. ground-based) network entity, the ARS field will indicate the fixed routing domain within which that network entity is located.

Note 2.— In the case of a mobile (i.e. aircraft-based) network entity, the ARS field will indicate the identity of the mobile (i.e. aircraft) routing domain within which that network entity is located.

4.5.6.1 Format

The format of the ARS field shall be as given in 4.5.6.1.1, 4.5.6.1.2, or 4.5.6.1.3, based on the authority responsible for the associated ATN Administrative Domain, and based on the value of the VER field.

4.5.6.1.1 ATSC-Fixed Format

The ATSC-Fixed ARS field shall contain the six-digit hexadecimal code for an ATN routing domain ~~identifier~~, when a ‘‘**Fixed**” VER value is present.

Note.— An ATSC administration may opt to derive six-digit hexadecimal ATSC-Fixed ARS field value syntax from the IA-5 encoding of the three least-significant characters of a four-character alphabetic symbol representing an appropriate ICAO Location Indicator.

4.5.6.1.2 AINSC-Fixed Format

The AINSC-Fixed ARS field shall contain the six-digit hexadecimal code for an ATN routing domain ~~identifier~~, when a ‘‘**Fixed**” VER value is present.

Note.— An AINSC administration may opt to derive six-digit hexadecimal AINSC-Fixed ARS field value syntax from the IA-5 encoding of a three-character alphabetic symbol representing an appropriate IATA Location Identifier.

4.5.6.1.3 Mobile Format

The Mobile-ARS field shall contain a six-digit hexadecimal number representing the 24-bit ICAO Aircraft Identifier, when a ‘‘**Mobile**” VER value is present.

4.5.6.2 Administration

ARS field values shall be administered by the authority given in 4.5.6.2.1, 4.5.6.2.2, or 4.5.6.2.3, based on the value of the VER field.

4.5.6.2.1 ATSC-Fixed Administration

ATSC ARS values shall be assigned and administered by ICAO.

Note.— Authority may be further delegated to State authorities as required.

4.5.6.2.2 AINSC-Fixed Administration

AINSC ARS values shall be assigned and administered by IATA.

Note.— Authority may be further delegated to aeronautical industry authorities as required.

4.5.6.2.3 Mobile Administration

Mobile ARS values shall be assigned and administered by ICAO.

Note.— Authority may be further delegated to State authorities as required.

4.5.6.3 Range

ARS field values shall be in the range **[000000]-[ffffff]**, expressed as hexadecimal numbers.

4.5.6.4 Encoding

The ARS field shall be encoded using binary rules, as defined in 4.4.5.

4.5.6.5 Default Value

If an ATN administrative domain chooses not to allocate fixed ARS field values (i.e. chooses not to partition the administrative domain into routing domains), then the value of the ARS field for all fixed addresses within that ATN administrative domain shall be **[000001]**. No default ARS field value shall be defined or allowed for mobile routing domains.

4.5.7 Location Identifier

The Location Identifier (LOC) field shall be used for partitioning the address space administered by a single ATN routing domain authority into more than one routing area.

4.5.7.1 Format

The format of the LOC field shall be as given in 4.5.7.1.1, 4.5.7.1.2 or 4.5.7.1.3, based on the authority responsible for the associated ATN Administrative Domain, and based on the value of the VER field.

4.5.7.1.1 ATSC Format

The ATSC-Fixed LOC field shall contain the four-digit hexadecimal code for an ATN routing area identifier, when an ‘‘**ATSC**” ADM value is present in combination with a ‘‘**Fixed**” VER value.

Note.— An ATSC administration may opt to derive four-digit hexadecimal ATSC LOC field value syntax from the three least-significant characters of a four-character identifier meta-character representing appropriate ICAO Location Indicators, encoded using ordinal rules defined in 4.4.7.

4.5.7.1.2 AINSC Format

The AINSC-Fixed LOC field shall contain the four-digit hexadecimal code for an ATN routing area identifier, when an ‘‘**AINSC**” ADM value is present in combination with a ‘‘**Fixed**” VER value.

Note.— An AINSC administration may opt to derive four-digit hexadecimal AINSC LOC field value syntax from a three-character identifier meta-character representing appropriate IATA Location Identifiers, encoded using ordinal rules defined in 4.4.7.

4.5.7.1.3 Mobile Format

The Mobile-LOC field shall contain the four-digit hexadecimal code for an ATN routing area identifier, when a ‘‘**Mobile**” VER value is present.

4.5.7.2 Administration

LOC field values shall be administered by the authority designated in the ADM field.

4.5.7.3 Range

LOC field values shall be in the range **[0000]-[ffff]**, expressed as hexadecimal numbers.

4.5.7.4 Encoding

The LOC field shall be encoded using binary rules, as defined in 4.4.5.

4.5.7.5 Default Value

If an ATN routing domain administration chooses not to allocate LOC field values (i.e. chooses not to partition the routing domain into routing areas), then the value of the LOC field for all addresses within that ATN routing domain shall be **[0001]**.

4.5.8 System Identifier

The System Identifier (SYS) field shall identify the end-system or intermediate-system containing the addressed Network entity.

4.5.8.1 Format

The format of the SYS field shall be determined by the authority designated in the ADM field.

4.5.8.2 Administration

The SYS field shall be administered by the authority designated in the ADM field.

4.5.8.3 Range

SYS field values shall be in the range **[000000000000]-[fffffffffff]**, expressed as hexadecimal numbers.

4.5.8.4 Encoding

The SYS field shall be encoded using binary rules, as defined in 4.4.5.

4.5.9 NSAP Selector

The NSAP Selector (SEL) field shall identify the end-system or intermediate-system network entity or network service user process responsible for originating or receiving Network Service Data Units (NSDUs).

4.5.9.1 Format

The SEL field shall contain the two-digit hexadecimal representation of a network entity or network service user protocol selector.

4.5.9.2 Administration

SEL field values in the range [01] - [fd] shall be assigned and administered by the authority designated in the ADM field.

Note. — Authority may be further delegated by the designated authority as required.

4.5.9.3 Range

Valid SEL field values shall be in the range **[00-ff]**.

The SEL field value for an intermediate-system network entity shall be [00], except for the case of an airborne intermediate-system not supporting IDRP. In that case, the SEL field value shall be [fe]. The SEL field value [ff] shall be reserved.

Note. — SEL values in stand-alone end-systems (i.e.in end-systems not co-located with intermediate-systems) are not constrained.

4.5.9.4 Encoding

The SEL field shall be encoded using binary rules, as defined in 4.4.5.

4.6 Transport Layer Addressing

4.6.1 General

Note 1.— This section provides requirements on the format of ATN TSAP addresses. An ATN TSAP address is an NSAP address and a TSAP selector.

Note 2.— The requirements in this section apply to the administration of transport addresses local to an ATN End System. They do not apply to all systems in a global OSI Environment. An ATN System may allow remote transport addresses to obey different standards, e.g. when interworking with a non-ATN system is required.

4.6.2 ATN TSAP Selector

An ATN TSAP selector shall be either one or two octets in length.

4.6.3 Format

The TSAP Selector field shall be interpreted as an unsigned binary integer.

4.6.4 Administration

The TSAP Selector field shall be administered on a local basis.

4.6.5 Range

Valid ATN TSAP Selector field values shall be in the range **[0] - [65535]**.

4.6.6 Encoding

The TSAP Selector field shall be encoded using binary rules, as defined in 4.4.5.

Recommendation.— *TSAP selector values in the range **[0] - [255]** should be encoded using one octet, higher values should be encoded using two octets.*

5. TRANSPORT SERVICE AND PROTOCOL SPECIFICATION

5.1 General

1. The COTP shall be used to provide an end-to-end reliable data transfer service between transport service users on two ATN ESs.
2. In ATN ESs, the implementation of the COTP shall conform to ISO 8073:1992 and the mandatory requirements given in this chapter.
3. The CLTP shall be used to provide a CL data transfer service between TS-users on two ATN ESs.
4. In ATN ESs, the implementation of the CLTP shall conform to ISO 8602 and the mandatory requirements given in this chapter.

Note.— The transport protocols specified for use in ATN ESs provide both CO and CL communication services. The implementation and use of a particular mode of the transport layer service depends on the requirements of the application(s) supported by a given ATN ES.

5.1.1 References

1. ISO/IEC 8073:1992 Information Technology - Telecommunications and Information Exchange between Systems - Open Systems Interconnection - Protocol for providing the Connection-mode Transport Service
2. ISO/IEC 8602 Information Processing Systems - Open Systems Interconnection - Protocol for providing the Connectionless-mode Transport Service.

5.1.2 Transport~~Internet~~ Service Description

Note 1. — When the TS-USER requires use of the connection mode transport protocol the TS-USER will provide the following information to the TS-PROVIDER on a per Transport Connection basis:

a) called and calling TSAP address;

b) whether or not the expedited data option is required;

c) the required residual error rate (RER) to determine whether or not the transport checksum is required;

d) the Application Service Priority to be mapped into the resulting CLNP NPDUs according to Table 2-2;

e) the ATN Security Label specifying the ATN Traffic Type, i.e.

- *ATN Operational Communications;*
- *ATN Administrative Communications;*
- *General Communications;*
- *Systems Management Communications.*

In the case where the Traffic Type specified is ATN Operational Communications the TS-USER will additionally provide the Sub-type, i.e. Air Traffic Services Communications (ATSC) or Aeronautical Operational Control Communications (AOCC).

In the case of the ATSC sub-type the TS-USER will further specify the required Class of Communications Service from Class A to Class H.

In the case of the AOCC sub-type the TS-USER will further specify the subnetwork preference (including no preference).

The ATN Traffic Types and their associated Sub-types are specified in Chapter 6, Table 6-1. The encoding of the ATN Security Label is specified in Chapter 6, Figure 6-1 and section 6.2.2.1 bullet 2.

Note 2. — The TS-USER is not required to specify any other Transport Service Quality of Service parameters.

5.1.3 Transport Service Access Point Addresses

1. A TSAP address shall comprise two elements, a NSAP address and a TSAP selector.
2. The NSAP address and the TSAP selector shall conform to the provisions in Chapter 4.

5.1.4 Network Service Specification

1. The COTP shall operate using the CLNS as specified in Chapter 6.

Note.— TPDUs are sent via the N-UNITDATA Request primitive.

5.1.5 Exchange of Transport-Selector parameters

Note 1. — TSAP Selectors are transmitted in Calling and Called Transport-Selector parameters in COTP, and in Source and Destination Transport-Selector parameters in CLTP.

The transport entity shall support Transport-Selector parameters to accomodate the ATN TSAP selector syntax and encoding requirements as specified in Chapter 4.

Recommendation.— The transport entity should support remote Transport-Selector parameters of variable size from 0 up to 32 octets using any encoding and any value.

Note 2. — The absence of a Calling and Called Transport-Selector assumes the Network Address alone unambiguously defines the Transport Address.

In COTP, on receipt of CR TPDU, the absence of a Calling or Called Transport-Selector shall be treated as equivalent to a zero length Calling or Called Transport-Selector. The absence of a Calling or Called Transport-Selector in a received CC TPDU shall indicate that Calling or Called Transport-Selector is equivalent to the corresponding parameter specified in the sent CR TPDU. When present in a received CC TPDU, Calling and Called Transport-Selector parameters shall be identical in length and value to the corresponding parameter specified in the sent CR TPDU.

In CLTP, on receipt of UD TPDU, the absence of a Source or Destination Transport-Selector shall be treated as equivalent to a zero length Source or Destination Transport-Selector.

5.2 Connection Mode Transport Layer Operation

5.2.1 Connection Mode Transport Protocol Overview

ATN ESs shall implement the ISO 8073 Class 4 transport protocol in order to provide CO communications over the ATN internetwork.

Note.— The ATN COTS model conforms to the model defined in ISO 8072.

5.2.2 Connection Mode Transport Quality of Service

5.2.2.1 Connection Mode Transport Priority

1. The transport layer shall allow a TS-user to specify priority in the range **[0 - 14]**.
2. The transport layer shall not alter the proposed TC priority specified by the TS-user.
3. The transport layer shall treat all connections without expressed priority as being at the default priority
4. The default priority shall be the lowest priority [**14**].
5. When a TS-user specifies a transport connection priority, the relationship between this transport connection priority and the CLNP~~network~~ priority shall be as specified in Table 2-3~~2~~.

5.2.2.2 Connection Mode Transport Security

Note.— The ATN security mechanism does not make use of the ISO/IEC 8073 Protection parameter. The support of the Protection parameter is therefore optional for CNS/ATM-1 Package.

The transport layer shall allow a TS-user to specify a Security Label for a transport connection. The transport security shall be implemented as specified in 2.7.3.1. The Security Label shall be encoded according to the provisions of Chapter 6, section 6.2.2.1. The transport layer shall not alter the Security Label specified by the TS-user.

The transport layer shall treat all connections without expressed security as default security.

The default security shall be the zero-length Security Label value indicating « General Communications » traffic.

Note.— When default security label is specified, NPDUs are generated without CLNP Security parameter.

5.2.3 Connection Mode Transport Service Primitives

Note 1. — For the purpose of describing the notional interfaces between different OSI protocol layers, each protocol layer is assumed to provide a service to the next higher protocol layer. The assumed service provided by the OSI transport layer to its user is described in ISO 8072.

Note 2. — ATN Applications may specify their use of the COTP implemented in ATN ESs using the TS specified in ISO 8072 including use of, priority,

and security parameters as specified in this specification.

Note 3. — There is no requirement to implement ISO 8072 as a software interface.

5.2.4 Connection Mode Transport APRL

5.2.4.1 Mandatory and Optional Functions

Note. — The requirements for the COTP are provided in the form of an ATN Profile Requirements List (APRL). The APRL has been prepared using the PICS proforma provided with ISO 8073. The APRL conventions are described in Part 1 of the CNS/ATM-1 Package SARPs.

An implementation of the ISO 8073 Transport Protocol shall be used in an ATN ES if and only if its PICS is in compliance with the APRL provided with these SARPs.

5.2.4.1.1 Protocol Implementation

5.2.4.1.1.1 Classes Implemented

The ATN COTP shall implement the features marked "M" in the table.

Index	Class	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
C0	Class 0	14.2	O.1	O
C1	Class 1	14.4	C0:O	O
C2	Class 2	14.2	O.1	O
C3	Class 3	14.3	C2:O	O
C4	Class 4 operation over CONS	14.3	C2:O	O
C4L	Class 4 operation over CLNS	14.3	C2:O	M

5.2.4.1.1.2 Specific ATN Requirements.

The CNS/ATM-1 ATN COTP shall implement the features marked "M" in the table.

Index	Feature	CNS/ATM-1 Package Support
ATN1	Initiating CR TPDU?	M
ATN2	Responding to CR TPDU?	M
ATN3	Extended TPDU Numbering	O
ATN4	Acceptance of Non-use of Checksum?	M
ATN5	Use of Concatenation?	O
ATN6	Use of Selective Acknowledgement?	O
ATN7	Use of Request of Acknowledgment?	O
ATN8	Reduction of Credit Window	M
ATN9	ER TPDU Transmission?	O
ATN10	Use of Called Transport-Selector Parameter in CR TPDU?	M
ATN11	Use of Calling Transport-Selector Parameter in CR TPDU?	M
ATN12	Use of TPDU Size Parameter in CR TPDU?	O
ATN13	Use of the Additional Option Selection Parameter in CR TPDU?	M
ATN14	Use of the Priority Parameter in CR TPDU?	M
ATN15	Use of the Acknowledgment Timer Parameter in CR TPDU?	M
ATN16	Use of Preferred Maximum TPDU Size Parameter in CR TPDU?	O
ATN17	Use of Inactivity Time Parameter in CR TPDU?	M
ATN18	Use of Called Transport-Selector Parameter in CC TPDU?	M
ATN19	Use of Calling Transport-Selector Parameter in CC TPDU?	M
ATN20	Support of TPDU Size Parameter in CC TPDU?	O

Index	Feature	CNS/ATM-1 Package Support
ATN21	Use of the Additional Option Selection Parameter in CC TPDU?	M
ATN22	Use of the Priority Parameter in CC TPDU?	M
ATN23	Use of the Acknowledgment Timer Parameter in CC TPDU?	M
ATN24	Use of Preferred Maximum TPDU Size Parameter in CC TPDU?	O
ATN25	Use of Inactivity Time Parameter in CC TPDU?	M
ATN26	1024 octets as the minimum preferred maximum TPDU size in a CR TPDU?	O
ATN27	1024 octets as the minimum preferred maximum TPDU size in a CC TPDU?	O
ATN28	1024 octets as the largest value of the maximum TPDU size parameter in a CR TPDU with preferred class 4?	O
ATN29	1024 octets as the largest value of the maximum TPDU size parameter which may be sent in a CC TPDU when class 4 is selected?	O
ATN30	Congestion Avoidance Measures?	M
ATN31	Quality of Service Mapping?	O
ATN32	Timer Settings?	M

Note.- ATN 31 refers to:

a) the passing of the CE bit and the security parameter between the transport and the network entity and

b) the mapping of the priority value between the transport and the network entity

5.2.4.1.2 Initiator/Responder Capability for Protocol Classes 0-4

The ATN transport protocol shall implement the features marked " M" in the table.

Index		ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
IR1	Initiating CR TPDU	14.5 a)	O.2	M
IR2	Responding to CR TPDU	14.5 a)	O.2	M

Note. — ISO 8073 requires that at least one of these options shall be implemented.

5.2.4.1.3 Supported Functions

5.2.4.1.3.1 Supported Functions for Class 4 (C4 OR C4L::).

5.2.4.1.3.1.1 Mandatory Functions for Class 4.

The ATN COTP shall implement the features marked "M" in the table.

Index	Function	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
T4F1	TPDU transfer	6.2	M	M
T4F2	Segmenting	6.3	M	M
T4F3	Reassembling	6.3	M	M
T4F4	Separation	6.4	M	M
T4F5	Connection establishment	6.5	M	M
T4F6	Connection refusal	6.6	M	M
T4F7	Data TPDU numbering (normal)	6.10	M	M
T4F8	Retention and acknowledgement of TPDUs (AK)	6.13.4.1	M	M
T4F9	Explicit flow control	6.16	M	M
T4F10	Checksum	6.17	M	M
T4F11	Frozen references	6.18	M	M
T4F12	Retransmission on time-out	6.19	M	M
T4F13	Resequencing	6.20	M	M
T4F14	Inactivity control	6.21	M	M

5.2.4.1.3.1.2 Mandatory Functions for Operation over Connectionless Network Service.

The ATN COTP shall implement the features marked "M" in the table.

Index	Function	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
T4F23	Transmission over CLNS	6.1.2	M	M
T4F24	Normal release when operating over CLNS (explicit)	6.7.2	M	M
T4F25	Association of TPDUs with transport connections when operating over CLNS	6.9.2	M	M
T4F26	Expedited data transfer when operating over CLNS (Network normal)	6.11.2	M	M
T4F27	Treatment of protocol errors when operating over CLNS	6.22.2	M	M

5.2.4.1.3.1.3 ISO 8073 Optional Functions.

The ATN COTP shall implement the features marked "Predicate:M" in the table if the predicate is true, i.e. the ATN recommendation has been followed.

Index	Feature	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
T4F28	Data TPDU numbering (extended)	6.10	O	ATN3:M
T4F29	Non-use of checksum	6.17	O	ATN4:M
T4F30	Concatenation	6.4	O	ATN5:M
T4F31	Retention and acknowledgement of TPDUs Use of selective acknowledgement	6.13.4.3	O	ATN6:MO
T4F32	Retention and acknowledgement of TPDUs Use of request acknowledgement	6.13.4.2	O	ATN7:MO

T4F30:: The transport entity shall not concatenate TPDUs from TCs with different transport priorities or different security types.

T4F31:: **Recommendation.—** *The Selective Acknowledgement should be used for conservation of bandwidth by preventing retransmission of correctly received out-of-sequence TPDUs.*

T4F32:: **Recommendation.—** *The Request of Acknowledgement should be used to reduce AK traffic*

Note.- The classification "MO" indicates mandatory to implement, optional to use.

5.2.4.1.4 Supported TPDUs

The ATN COTP shall implement the features marked "M" in the table.

Index	TPDUs		ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
ST1	CR	supported on transmission	13.1	IR1:M	M
ST2	CR	supported on receipt	13.1	IR2:M	M
ST3	CC	supported on transmission	13.1	IR2:M	M
ST4	CC	supported on receipt	13.1	IR1:M	M
ST5	DR	supported on transmission	13.1	IR2:M	M
ST6	DR	supported on receipt	13.1	IR1:M	M
ST7	DC	supported on transmission	13.1	C4L:M	M
ST8	DC	supported on receipt	13.1	C4L:M	M
ST9	DT	supported on transmission	13.1	M	M
ST10	DT	supported on receipt	13.1	M	M
ST11	ED	supported on transmission	13.1	C4L:M	MO
ST12	ED	supported on receipt	13.1	C4L:M	MO
ST13	AK	supported on transmission	13.1	C4L:M	M
ST14	AK	supported on receipt	13.1	C4L:M	M
ST15	EA	supported on transmission	13.1	C4L:M	MO
ST16	EA	supported on receipt	13.1	C4L:M	MO
ST19	ER	supported on receipt	13.1	M	M

Note.— The following table states for which classes, if any, ER TPDU is supported on transmission:

Index	Class	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
SER4L	Class 4 over CLNS	6.22.2	O	ATN9:M

5.2.4.1.5 Supported Parameters of Issued TPDUs

5.2.4.1.5.1 Parameter Values for CR TPDU (C4L::)

If the additional options selection parameter is issued in a CR TPDU it is mandatory that:

Index		ISO/IEC 8073 Reference
ICR1	Bits 8 to 7 shall be set to zero	13.3.4 g)

If the preferred class in the CR is 2,3 or 4:

Index		ISO/IEC 8073 Reference	ISO Status	CNS/ATM-1 Package Support
ICR2	Is class 0 always offered as an alternative class?	14.4	O	X

5.2.4.1.5.2 Supported parameters for Class 4 TPDUs (C4L::)

5.2.4.1.5.2.1 Optional Parameters for a Connection Request TPDU.

The ATN COTP shall implement the features marked "M" in the table.

Index	Supported parameters	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
I4CR7	Called Transport-Selector	13.3.4 a)	O	M
I4CR8	Calling Transport-Selector	13.3.4 a)	O	M
I4CR9	TPDU size	13.3.4 b)	O	ATN12:MO
I4CR10	Version Number	13.3.4 d)	O	O
I4CR11	Protection parameters	13.3.4 e)	O	O
I4CR12	Additional option selection	13.3.4 g)	O	M
I4CR13	Throughput	13.3.4 k)	O	O
I4CR14	Residual error rate	13.3.4 m)	O	O
I4CR15	Priority	13.3.4 n)	O	ATN14:M
I4CR16	Transit delay	13.3.4 p)	O	O
I4CR17	Acknowledgement time	13.3.4 j)	O	ATN15:M
I4CR18	Preferred maximum TPDU size	13.3.4 c)	O	ATN16:MO
I4CR19	Inactivity timer	13.3.4 r)	O	ATN17:M

I4CR9:: **Recommendation.**— *The transport layer should propose a TPDU size of 1024 octets or more*

Recommendation.— *The transport layer should use the TPDU size parameter rather than the preferred maximum TPDU size parameter.*

5.2.4.1.5.2.2 Optional Parameters for a Connection Confirm TPDU.

Note. — According to ISO, the following parameters are optional if a CC TPDU is issued in class 4:

Index	Supported parameters	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
I4CC6	Called Transport-Selector	13.4.4	O	M
I4CC7	Calling Transport-Selector	13.4.4	O	M
I4CC8	TPDU size	13.4.4	O	ATN20:M
I4CC9	Protection parameters	13.4.4	O	O
I4CC10	Additional option selection	13.4.4	O	M
I4CC11	Acknowledgement time	13.4.4	O	ATN23:M
I4CC12	Throughput	13.4.4	O	O
I4CC13	Residual error rate	13.4.4	O	O
I4CC14	Priority	13.4.4	O	ATN22:M
I4CC15	Transit delay	13.4.4	O	O
I4CC16	Preferred maximum TPDU size	13.4.4	I4CR18:O	ATN24:M
I4CC17	Inactivity timer	13.4.4	O	ATN25:M

I4CC10:: *Note.— The support of T4F26 implies that the Additional Options Selection parameter is mandatory.*

5.2.4.1.5.2.3 Optional Parameter for a Disconnect Request TPDU.

Index	Supported parameter	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
I4DR4	Additional information	13.5.4 a)	O	O

5.2.4.1.5.2.4 Mandatory Parameter for a Data TPDU

Note.— According to ISO, the following parameter is mandatory in a DT TPDU if request of acknowledgement has been selected.

Index	Supported parameter	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
I4DT4	ROA	13.7.3 b)	T4F32:M	T4F32:M

5.2.4.1.5.2.5 Optional Parameter for an Acknowledgement TPDU

Note.— According to ISO, an AK TPDU containing flow control information will be transmitted if an AK TPDU is received under the conditions specified in ISO 8073 12.2.3.9. The following parameter is mandatory if an AK TPDU is issued in Class 4.

Index	Supported parameter	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
I4AK4	Flow control confirmation	13.9.4 c)	O	M

5.2.4.1.5.2.6 Use of the Subsequence Number Parameter in the Acknowledgement TPDU

Note.— According to ISO, if an implementation can reduce credit and does so in the manner outlined in ISO 8073 12.2.3.8.2 then subsequence number in AK is mandatory.

Index	Supported parameters	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
I4AK5	Subsequence number	13.9.4. b)	O	ATN8:M

5.2.4.1.5.2.7 Use of the Selective Acknowledgement Parameter in the Acknowledgement TPDU

Note.— According to ISO, the following parameter is optional in an AK TPDU if selective acknowledgement has been negotiated.

Index	Supported parameter	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
I4AK6	Selective acknowledgement parameters	13.9.4. d)	T4F31:O	T4F31:O

5.2.4.1.5.2.8 Optional Parameters for an Error TPDU

Index	Supported parameter	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
I4ER3	Invalid TPDU	13.12.4 a)	O	O

5.2.4.1.6 Supported parameters for received TPDUs

Note.— ISO 8073 requires implementations to be capable of receiving and processing all possible parameters for all possible TPDUs, depending upon the class and optional functions implemented.

5.2.4.1.6.1 TPDUs in Class 4 (C4L::)

Note.— According to ISO, if use of checksum has been selected then it is mandatory to process a checksum parameter in the following TPDUs:

The ATN COTP shall implement the features marked "M" in the table.

Index	TPDU	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
R4CCch	CC TPDU	13.4.4	M	M
R4DRch	DR TPDU	13.5.4 b)	M	M
R4DCch	DC TPDU	13.6.4	M	M
R4DTch	DT TPDU	13.7.4	M	M
R4EDch	ED TPDU	13.8.4	M	M
R4AKch	AK TPDU	13.9.4 a)	M	M
R4EAch	EA TPDU	13.10.4	M	M
R4ERch	ER TPDU	13.12.4 b)	M	M

5.2.4.1.7 User Data in Issued TPDUs

5.2.4.1.7.1 Class 4 (C4 or C4L::)

The ATN COTP shall implement the features marked "M" in the table.

Index	User Data	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
D4ICR	User data of up to 32 octets in a CR with preferred class 4	13.3.5	M	M
D4ICC	User data of up to 32 octets in a CC	13.4.5	M	M
D4IDR	User data of up to 64 octets in a DR	13.5.5	M	M

5.2.4.1.8 User Data in Received TPDUs

The transport layer shall be able to receive the following:

Index	User Data	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
DRCC	32 octets of user data in a CC TPDU	13.4.5	IR1:M	IR1:M
DRDR	64 octets of user data in a DR TPDU	13.5.5	IR1:M	IR1:M
DRCR	32 octets of user data in a CR TPDU	13.3.5	IR2:M	IR2:M

5.2.4.1.9 Negotiation

Note.— If an option is not returned in the CC, it is considered to have been refused. This allows compatible negotiation between versions of the ISO 8073 transport protocol

5.2.4.1.9.1 Class Negotiation - Initiator

Index	Feature	ISO/IEC 8073 References	CNS/ATM-1 Package Supported Value
NC	The preferred class in the CR TPDU may contain any of the classes supported by the implementation	6.5.5 j)	Class 4

Note 1.— Negotiation of other protocol classes is out of scope. If this is the only profile supported then it is not possible to negotiate any other protocol class.

Note 2.— The table below specifies valid alternative classes

Index	Preferred class	ISO/IEC 8073 References	ISO Allowed values	CNS/ATM-1 Package Supported values
NAC5	Class 4 over CLNS	6.5.5 j)	None	None

NAC5:: *Note.— The class cannot be negotiated since Class 4 is the only class allowed over CLNS.*

5.2.4.1.9.2 Class negotiation - responder side

Index	Preferred class	ISO/IEC 8073 References	ISO Allowed responses	CNS/ATM-1 Package Supported values
RC4	What classes can you respond with if CR proposes only class 4?	6.5.4 j) Table 3	2,4 or connection refused depending on classes supported	4
RC4a	What classes can you respond with if CR proposes class 4 as preferred class and the alternative class parameter is present?	6.5.4 j) Table 3	0,1,2,3,4 or connection refused depending on classes supported and coding of alternative class	4

Note.— This table does not preclude connection refusal for other reasons.

5.2.4.1.9.3 TPDU Size Negotiation

Index	TPDU size	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
TS1	If maximum TPDU size is proposed in a CR TPDU then the initiator shall support all TPDU sizes from 128 octets to the maximum proposed, as defined in ISO 8073	14.6 e)	I4CR9:M	I4CR9:M
TS2	If the preferred maximum TPDU size parameter is used in a CR TPDU then the initiator shall support all TPDU sizes, except 0, that are multiples of 128 octets up to the preferred maximum proposed	14.6 e)	I4CR18:M	I4CR18:M

Index	TPDU size	ISO/IEC 8073 References	ISO Allowed values	CNS/ATM-1 Package Supported values
TS3	What is the largest value of the preferred maximum TPDU size parameter in a CR TPDU?	14.6 e)	any multiple of 128 octets	any multiple of 128 octets
TS4	What is the largest value of the preferred maximum TPDU size parameter in a CC TPDU?	14.6 e)	any multiple of 128 octets	any multiple of 128 octets

TS3, TS4:: *Note.— An implementation of the transport layer can support a preferred maximum TPDU size larger than 1024 octets.*

Index	TPDU size	ISO/IEC 8073 References	Allowed Values	CNS/ATM-1 Package Supported Values
T4S1	What is the largest value of the maximum TPDU size parameter in a CR TPDU with preferred class 4?	14.6 e)	One of 128, 256, 512, 1024, 2048, 4096, 8192	One of 128, 256, 512, 1024, 2048, 4096, 8192
T4S2	What is the largest value of the maximum TPDU size parameter which may be sent in the CC TPDU when class 4 is selected?	14.6 e)	128, 256, 512, 1024, 2048, 4096, 8192	128, 256, 512, 1024, 2048, 4096, 8192

TS3, TS4, T4S1, T4S2:: **Recommendation.**- *To support efficient transmission of anticipated application data exchanges, aTPDU size resulting from TPDU size negotiation (using either the maximum TPDU size or the preferred maximum TPDU size parameters) of at least 1024 octets is recommended.*

5.2.4.1.9.4 Use of Extended Format.

Index	Extended format	ISO/IEC 8073 References	ISO Allowed Values	CNS/ATM-1 Package Supported Value
NEF3	What formats can you propose in the CR TPDU in class 4?	6.5.5 n)	normal, extended	normal,extended
NEF6	What formats can you select in CC when extended has been proposed in CR in class 4?	6.5.5 n)	normal, extended	normal,extended

NEF3:: **Recommendation.**— *Implementations of the ATN transport layer should propose use of normal format in the CR TPDU.*

NEF3:: *Note.— Because the increased TPDU size resulting from use of extended data TPDU numbering may be more inefficient, this option should be used on a TC only when absolutely required.*

NEF3, NEF6:: *Note.— This table does not preclude proposal of the extended format.*

5.2.4.1.9.5 Expedited data Transport service

The ATN COTP shall implement the feature marked "M" in the table.

Note. — Use of the feature is optional.

Index	Expedited data	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Supported values
TED1	Is the expedited data indication supported in CR and CC TPDU?	6.5.5 r)	M	MO

TED1:: *Note.— Expedited data is proposed using the Additional Options Parameters in the CR and CC TPDUs.*

5.2.4.1.9.6 Non-use of Checksum (C4L and T4F29::).

Index	Non-use of checksum	ISO/IEC 8073 References	ISO Allowed Values	CNS/ATM-1 Package Supported Values
NUC1	What proposals can you make in the CR?	6.5.5 p)	non-use, use	non-use, use
NUC2	What proposals can you make in CC when non-use of checksum has been proposed in CR?	6.5.5 p)	non-use, use	non-use, use

NUC1:: *Note.— A transport layer is able to propose either use or non-use of checksum in a CR TPDU.*

NUC2:: *Note.— The term ”non-use” means that the transport layer may respond accepting non-use of checksum. A transport layer may also respond with use of checksum if non-use has been proposed.*

NUC2:: **Recommendation.**— *The transport layer should accept non-use of checksum when proposed in a CR TPDU.*

5.2.4.1.9.7 Use of selective acknowledgement

Index	Selective Acknowledgement	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
USA1	Is use of selective acknowledgement proposed in CR TPDUs ?	6.5.5 s)	O	ATN6:M
USA2	Is use of selective acknowledgement selected in a CC when it has been proposed in a CR ?	6.5.5 s)	O	ATN6:M

5.2.4.1.9.8 Use of Request Acknowledgement

Index	Request of Acknowledgement	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
ROA1	Is use of request of acknowledgement proposed in CR TPDUs ?	6.5.5 t)	O	ATN7:M
ROA2	Is use of request of acknowledgement selected in a CC when it has been proposed in a CR ?	6.5.5 t)	O	ATN7:M

5.2.4.1.10 Error Handling

Note.— Using Class 4 over CLNS, a TPDU with an invalid checksum will be discarded.

5.2.4.1.10.1 Action on Detection of a Protocol Error

Index	Item	ISO/IEC 8073 References	Values	
			ISO Allowed	CNS/ATM-1 Package Supported
PE4L	Class 4 over CLNS	6.22.2	ER, DR, Discard	ER, DR, Discard

PE0-PE3:: Note.— N/A

PE4L:: *Note.— The choice of action (DR, Discard) is an implementation choice and may depend on the type of error encountered.*

5.2.4.1.10.2 Actions on receipt of an invalid or undefined parameter in a CR TPDU

The ATN COTP shall implement the features marked "M" in the table.

Index	Event	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
RR1	A parameter not defined in ISO 8073 shall be ignored	13.2.3	M	M
RR2	An invalid value in the alternative protocol class parameter shall be treated as a protocol error	13.2.3	M	M
RR3	An invalid value in the class and option parameter shall be treated as a protocol error	13.2.3	M	M
RR4	On receipt of the additional option selection parameter bits 8 to 7, and bits 6 to 1 if not meaningful for the proposed class, shall be ignored	13.3.4 g)	M	M
RR6	On receipt of the class option parameter bits 4 to 1 if not meaningful for the proposed class shall be ignored	13.3.3 h)	M	M

Index	Event	ISO/IEC 8073 Reference	Value	
			ISO Allowed	CNS/ATM-1 Package Supported
RR7	A parameter defined in ISO 8073 (other than those covered above) and having an invalid value	13.2.3	Ignore, Protocol Error	Ignore, Protocol Error

RR7:: *Note.— The choice of action (Ignore, Protocol error) is an implementation choice and may depend on the type of error encountered.*

5.2.4.1.10.3 Actions on receipt of an invalid or undefined parameter in a TPDU other than a CR TPDU

The ATN COTP shall implement the features marked "M" in the table.

Index	Event	ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
U11	A parameter not defined in ISO 8073 shall be treated as a protocol error	13.2.3	M	M
U12	A parameter which has an invalid value as defined in ISO 8073 shall be treated as a protocol error	13.2.3	M	M
U13 (class 4 only)	A TPDU received with a checksum which does not satisfy the defined formula shall be discarded	6.17.3	M	M

5.2.4.1.11 Class 4 Timers and Protocol Parameters

The ATN COTP shall implement the features marked "M" in the table.

Index		ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
TA1	T1 (Local Retransmission)	12.2.1.1.4	M	M
TA2	N (Maximum Transmission)	12.2.1	M	M
TA3	I_L (Inactivity Time)	12.2.1.1.7	M	M
TA4	W (Window Update)	12.2.1	M	M
TA5	L (Frozen Reference Time)	12.2.1.1.6	M	M

Index		ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support
ATN-TA1	R (Persistence)	12.2.1.1.5	O	O
ATN-TA2	M_{LR} (NSDU Lifetime)	12.2.1.1.1	O	O
ATN-TA3	M_{RL} (NSDU Lifetime)	12.2.1.1.1	O	O
ATN-TA4	E_{LR} (Maximum Transmission Delay)	12.2.1.1.2	O	O
ATN-TA5	E_{RL} (Maximum Transmission Delay)	12.2.1.1.2	O	O
ATN-TA6	A_L (Acknowledgement Time)	12.2.1.1.3	O	ATN15:M
ATN-TA7	A_R (Acknowledgement Time)	12.2.1.1.3	O	ATN15:M
ATN-TA8	I_R (Inactivity Time)	12.2.1.1.7	O	ATN17:M

Note. — According to ISO, the following applies to an implementation under test:

Index		ISO/IEC 8073 References	ISO Status	CNS/ATM-1 Package Support

OT9	Does IUT support optional timer TS2 when operating in class 4?	6.22.2.3	O	O

5.2.4.2 Encoding of Transport Protocol Data Units

The encoding of TPDUs shall conform to ISO 8073 for the COTP.

5.2.5 Use of the ATN Network Service

Note.— This section specifies how the COTP operates over the CLNS provided by the ATN network layer.

.

5.2.5.1 Use of the N-UNITDATA Request

The transport layer shall use the N-UNITDATA Request primitive, as defined in ISO 8073, to transmit TPDUs.

Note.— The way the parameters are exchanged between the transport entity and the Network Service is a local matter.

The length indication given to the network service shall be equal to the length of the TPDU(s).

Note.— The maximum size of each TPDU is restricted to the locally defined maximum NSDU size.

5.2.5.1.1 NS-user-data

Note.— Transport entities transmit TPDUs as NS-user-data of the N-UNITDATA Request primitive.

5.2.5.1.2 Network Service Access Point Addresses

Note.— The transport layer has knowledge of the source and destination address parameters only as octet strings.

5.2.5.1.3 Network Quality of Service

The COTP shall use the network QOS parameters as defined in the sections below.

5.2.5.1.3.1 Network Layer Priority.

The COTP shall use the network priority parameter to indicate the relative priority of a NSDU. When a transport priority has been specified, the value of network priority shall be determined based on the transport connection priority, as defined in Table 2-~~3~~2.

If the transport layer supports levels of TC priority greater than 14, TPDUs associated with the TC shall be transmitted using a network priority level of zero.

Note.— As specified in ISO 8073, the transport layer priority level zero is highest. ISO 8473 specifies zero as the lowest network priority and fourteen as the highest. Table 2-~~3~~2 provides a suitable mapping between these two schemes for use by ATN systems.

5.2.5.1.3.2 Network Layer Security.

Note.— The use of the network layer security is specified in 2.7.4.1.

5.2.5.2 Use of the N-UNITDATA Indication

The transport layer shall be capable of receiving TPDUs from the ATN network service using the N-UNITDATA indication primitive, as defined in ISO 8073.

Note.— The way the parameters are exchanged between the transport entity and the Network Service is a local matter.

5.2.5.2.1 NS-user-data

Note.— Transport entities receive TPDUs as NS-user-data of the N-UNITDATA Indication primitive..

5.2.5.2.2 Network Service Access Point Addresses

Note.— The source and destination address parameters supplied to the COTP by the CLNS via the N-UNITDATA primitive supports the ATN NSAP addressing plan as specified in Chapter 4.

5.2.5.2.3 Network Quality of Service

5.2.5.2.3.1 Network Layer Security.

Note.— The use of the network layer security is specified in 2.7.4.1.

5.2.5.2.3.2 Congestion Notification

The network layer shall indicate the value of the C/E bit contained in the QOS Maintenance Parameter.

5.2.6 Transport Layer Congestion Avoidance

Note 1.— The congestion avoidance mechanisms in the transport layer make use of the notification by the network layer of Congestion Experience

flags in received NPDUs. This mechanism allows transport entities to reduce the window, i.e. the number of DT TPDUs allowed to be sent without acknowledgement, when the proportion of NPDUs indicating congestion reaches a certain threshold.

Note 2.— Transport Congestion Avoidance measures are applicable to connection oriented transport service only.

Note 3.— The algorithm defined in this section is applied for each transport connection individually.

The transport entity shall implement the congestion avoidance algorithm defined in this section.

5.2.6.1 Advertised window

A transport entity that is receiving TPDUs shall provide the transport entity that is sending the TPDUs with the lower window edge and the size of the *advertised window (W)* by using the explicit flow control mechanisms specified in ISO/IEC 8073.

*Note.— The **advertised window** is the window advertised by the receiver of the data to the sender of the data. It indicates the number of DT TPDUs that the receiver is willing to accept.*

5.2.6.2 Receiving Transport Entity Congestion Avoidance

5.2.6.2.1 Initialisation of the advertised window

The initial value of the advertised window W_0 that will be advertised to the sending transport entity shall have a locally configurable upper bound. This initial window shall be sent to the sending transport entity in the first CDT field transmitted.

5.2.6.2.2 Sampling Period

The receiving transport entity shall maintain a fixed value for the size of the advertised window *W* during a sampling period. The sampling period ends after *2*W* DT TPDUs have been received by the receiving transport entity.

Note.— The end of a sampling period determines the beginning of the next sampling period. The size of the advertised window may be modified at the end of a sampling period.

5.2.6.2.3 Counting of Received TPDUs in a Sampling Period

The receiving transport entity shall maintain a count *N*, equal to the number of TPDUs received, and a count, *NC*, equal to the total number of TPDUs received with an indication that congestion is experienced. All types of TPDUs shall be included in the counts for *N* and *NC*.

5.2.6.2.4 Action upon the end of a Sampling Period

The receiving transport entity shall take the following actions at the end of each sampling period:

1. If the count *NC* is less than λ % of the count *N*, the receiving transport entity shall increase the size of the advertised window by adding 1 up to a maximum based on the local buffer management policy. Otherwise, it shall decrease the size of the advertised window by multiplying it by β. If the result of this multiplication has a decimal part, the new window size shall be the truncated to its integer value. The size of the advertised window shall not go to a value smaller than 1.
2. The counts *N* and *NC* shall be reset to 0.
3. The new window size shall be transmitted to the sending transport entity in accordance with the explicit flow control mechanisms specified in ISO/IEC 8073.

Note.— If the window size is reduced by this procedure, the transport entity may have to reduce credit gradually so as to avoid the reduction of the upper window edge.

5.2.6.3 Recommended algorithm values

***Recommendation**.— The value settings defined in the following table should be implemented:*

Name	Description	Recommended value/range
β	Window decrease factor	0.5 to 0.625
W_0	Initial window	1
λ	Congestion ratio	50 %

5.3 Connectionless Mode Transport Protocol Operation

5.3.1 Connectionless Mode Transport Protocol Overview

ATN ESs shall implement the ISO 8602 transport protocol in order to provide CL communications over the ATN internetwork.

Note.— The ATN CLTS model conforms to the service model defined in ISO 8072.

5.3.2 ATN Connectionless Mode Transport Quality of Service Parameters

Recommendation.— *The transport layer should support the dynamic selection of checksums on a per TSDU basis*

5.3.2.1 Priority

The transport entity providing the connectionless mode transport service shall allow a TS-user to specify TSDU priority in the range **[0-14].**

Note.— The CLTP itself does not support a priority field in the TPDU.

5.3.2.2 Security

The transport entity providing the connectionless mode transport service shall use the TSDU security label provided in the T-UNITDATA request as the value of the N-UNITDATA security parameter.

Note.— The CLTP itself does not support a security parameter field in the TPDU.

5.3.3 Connectionless Mode Transport Service Primitives

Note 1. — For the purposes of describing the notional interfaces between different OSI protocol layers, each protocol layer is assumed to provide a service to the next higher protocol layer. The assumed service provided by the OSI transport layer to its user is described in ISO 8072.

Note 2.- ISO 8072 limits CL user-data to a maximum of 63 488 octets per TSDU.

Note 3. — There is no requirement to implement ISO 8072 as a software interface.

5.3.3.1 T-UNITDATA Request

The source and destination Transport Addresses shall conform to the ATN Transport Layer Addressing provisions as specified in Chapter 4.

5.3.3.2 T-UNITDATA Indication

Note. — All of the associated parameter values are equal to the values passed to the TS provider via the T-UNITDATA Request primitive, except possibly the QOS parameter values.

5.3.4 Connectionless Mode Transport APRL

Note. — The requirements for the CLTP are provided in the form of an APRL. The APRL has been prepared using the PICS proforma provided with ISO 8602.

Before use in an ATN ES, the transport protocol implementor shall provide a completed PICS for the ISO transport protocol implementation, using the PICS proforma provided with ISO 8602, including any extensions to that proforma provided with this material. An implementation of the ISO 8602 Transport Protocol shall be used in an ATN ES if and only if its PICS is in compliance with the APRL provided with these SARPs.

5.3.4.1 Protocol Implementation

The CLTP shall operate over the CLNS provided by the ATN network layer, according to the provisions in 5.3.5.

5.3.4.2 Encoding of Transport Protocol Data Units

The encoding of TPDUs shall conform to ISO 8602 for the CLTP.

5.3.4.3 ATN Connectionless Transport Protocol APRL

The ATN CLTP shall implement the features marked "M" in the table.

Item	Protocol Function Support	ISO 8602 Clause	ISO Status	CNS/ATM-1 Package Support
NS	Network service selection	5.3.2.2	M	M
AM	Address mapping	5.3.2.3	M	M
	PDU Support			
UD1	Unitdata PDU supported on transmission	6.1.3	M	M
UD2	Unitdata PDU supported on reception	6.1.3	M	M
	Parameters of the Unitdata PDU on Transmission			
TpTc	<t> TPDU UD Checksum	6.2.4.1	O	M
TpTs	<t> TPDU UD Source Transport-Selector	6.2.4.1	M	M
TpTd	<t> TPDU UD Destination Transport-Selector	6.2.4.1	M	M
TpTu	<t> TPDU UD User Data	6.2.4.1	O	M
	Parameters of the Unitdata PDU on Reception			
TpRc	<r> TPDU UD Checksum	6.2.4.2	M	M
TpRs	<r> TPDU UD Source Transport-Selector	6.2.4.2	M	M
TpRd	<r> TPDU UD Destination Transport-Selector	6.2.4.2	M	M
TpRu	<r> TPDU UD User Data	6.2.4.2	M	M
	Service Support			
CL	Connectionless Mode Network Service	6.2	M	M

5.3.5 Use of the ATN Network Service

Note.— This section specifies how the CLTP operates over the CLNS provided by the ATN network layer.

5.3.5.1 General

The CLTP shall use the NS primitives described in Chapter 6 for the transmission and reception of TPDUs.

Note.— The method of parameter exchange between the TE and the NS is a local matter.

5.3.5.2 Use of the N-UNITDATA Request

The transport layer shall use the N-UNITDATA Request Primitive, as defined in ISO 8602, to transmit TPDUs.

5.3.5.2.1 NS-user-data

The length indicated shall be no different from the length of the TPDU(s).

Note.— *TEs transmit TPDUs as NS-user-data of the N-UNITDATA Request primitive.*

5.3.5.2.2 Network Service Access Point Addresses

Note. — The transport layer has knowledge of source and destination address parameters only as octet strings.

5.3.5.2.3 Network Quality of Service

The transport entity providing the connectionless mode transport service shall use the network QOS parameters as defined in the sections below.

5.3.5.2.3.1 Network Layer Priority

The transport entity providing the connectionless mode transport service shall use the network priority parameter to indicate the relative priority of an NSDU. The NSDU priority shall be determined from the TSDU priority, using the mapping given in Table 2-3~~2~~.

5.3.5.2.3.2 Network Layer Security

The transport entity providing the connectionless mode transport service shall use the security label provided in the T-UNITDATA request as the value of the N-UNITDATA security parameter.

5.3.5.3 Use of the N-UNITDATA Indication

Note.— Following ISO 8602, the transport layer receives TPDUs from the network-layer-provided N-UNITDATA Indication primitive.

5.3.5.3.1 Network Service Access Point Addresses

Note.— The source and destination address parameters supplied to the CLTP by the NS via the N-UNITDATA Indication primitive supports the ATN NSAP addressing plan as specified in Chapter 4.

5.3.5.3.2 Network Quality of Service

To meet the ISO 8072 service specification, the transport entity providing the connectionless mode transport service shall translate application service priority to network layer priority, and shall perform the inverse operation on reception, using the mapping shown in Table 2-3~~2~~.

5.4 Implementation

Recommendation. — *The following timers and variables should be configurable on a TC basis:*

- *the local retransmission timer (T1),*
- *the acknowledgement timer (A_L),*
- *the window update timer (W),*
- *the inactivity timer (I),*
- *the frozen reference time (L),*
- *the maximum retransmission number (N),*
- *the persistence timer (R)*

For use in the ATN, the acknowledgement timer (A_L) shall retain the ISO 8073 standard parameter length of 2 octets (16 bits) but express the value in seconds (rather than milliseconds). A maximum value of 65,565 seconds for this Acknowledgment Timer is therefore allowed for use within the ATN.

Note 1 .— This change is in response to the unique requirements of the aeronautical environment which may require longer acknowledgment times.

Note 2. — Initial values of these timers will be dependant upon the traffic type and routing policy requirements expressed in the associated ATN Security Label.

Note 3. — Implementors are advised to permit systems administrators to readily specify such initial values.

6. INTERNETWORK SERVICE AND PROTOCOL SPECIFICATION

6.1. Introduction

The ATN network comprises a number of interconnected ATN routers and constituent subnetworks supporting packet data communication among host computers operating the ATN internet protocols.

All ATN NPDUs (packets) are encapsulated within appropriate subnetwork protocol data units for transfer among ATN network entities using the connectionless ISO OSI network layer service provided by the ATN internet. As all ATN internet protocols are connectionless, any information required to process a particular NPDU must be carried within the header of that network protocol data unit for processing by ATN routers and host computers.

6.1.1. Scope

This chapter provides requirements and recommendations pertaining to the use of the ISO 8473 by ATN ES and IS Network entities. This chapter is concerned with the use of ISO 8473 in the context of the internetworking protocol approach to the provision of CLNS as defined in ISO/IEC 8348. This chapter contains ATN-specific protocol implementations and is concerned with the interoperability of protocol implementations. It therefore provides appropriate compliance statements and APRLs for this purpose.

The ATN Network Layer connectionless-mode network service supports the transfer of a connectionless network service data unit (NSDU) from a source NSAP to a destination NSAP within the ATN network. Each such NSDU transfer is the result of a single invocation of the connectionless-mode Network Service encompassed within the ATN.

6.1.2. Applicability of Requirements

All ATN IS and ES Network entities shall comply with the provisions contained in sections 6.2, ATN Specific Features and 6.3, Mandatory and Optional Functions, in addition to all APRLs specified in section 6.4.

6.2. ATN Specific Features

6.2.1. Purpose of ATN Specific Features

Note 1.— The ATN infrastructure, referred to as an internet, comprises the interconnection of computers with gateways and routers via real subnetworks. This internetworking infrastructure, developed by ICAO, allows for the incorporation of differing air-to-ground and ground-to-ground subnetworks servicing differing user groups, i.e., air traffic services (ATS), aeronautical operational control (AOC), and others.

Note 2.— The CLNP protocol used to operate this internetworking infrastructure is based on ISO/IEC 8473 with ATN-specific additions to reflect the unique communications environment of the ATN.

Note 3.— The ATN specific functions listed in this chapter reflect responses to the additional functional needs of ATN Network entities in order to support user requirements concerned with:

a) Ensuring that information is conveyed about Traffic Type and Routing Policy requirements pertaining to user data in NPDUs;

b) Ensuring that a priority scheme can be applied for management of ES and IS output queues and buffers;

c) Ensuring that specific policies and procedures are available to handle congestion avoidance and congestion control requirements within the ATN.

6.2.2. The Security Function

The SECURITY Function shall be supported by ATN ES or IS Network entity implementations receiving or transmitting inter-domain traffic other than General Communications. ATN Network entities shall therefore provide the Globally Unique Security format for all created NPDUs.

The sole exception to this requirement is for General Communications traffic where no Security parameter information is required to be encoded in created NPDUs.

6.2.2.1. Encoding of the Security Parameter

The CLNP Options Security Parameter is used in the ATN to convey information about the Traffic Type and Routing Policy Requirements pertaining to the user data of the NPDU (other than General Communications). It may also be used to convey a security classification.

The value component of the CLNP Options Security Parameter shall be encoded as follows:

1. The first octet shall always be encoded as [**1100 0000]** to indicate the Globally Unique Security Format
2. The remaining octets shall contain the ATN Security Label encoded as the four fields illustrated in Figure 6-1, and defined below.

	Security Registration ID Length	Security Registration ID (variable)	Security Information Length	Security Information (optional)
Octet	0	1	n	n+1

Figure 6-1: The ATN Security Label

Note.— The Security Registration ID identifies the authority that has specified the associated security policy.

6.2.2.2. Security Registration ID Length

This field shall be one octet long and contain the length in octets of the Security Authority's Security Registration Identifier.

6.2.2.3. Security Registration ID

This variable field shall contain a Security Type object identifier encoded using ASN.1 Basic Encoding Rules with the following sequence of integer values:

{1 3 27 0 0} The ATN Security Registration Identifier

Note.— The ATN Security Registration Identifier identifies the ATN Security Authority. ICAO has been assigned an International Code Designator (ICD) decimal value [00027] in accordance with the dictates of ISO 6523. According to ISO 6523 and ISO 8824 this value identifies an arc of the identified organisation of ISO. ICAO object identifiers designate an ICAO defined hierarchy starting with {1 3 27}. Under this arc, {0} has been designated as ATN, and the flat address space under ATN starts with object identifiers {0,1,2,3,4, ...}. Value {0} has been assigned as the Traffic Type and Routing Policy identifier.

6.2.2.4. Security Information Length

This field shall be one octet in length and shall indicate the length in octets of the Security Information. If there is no security information, this field shall indicate a zero length.

6.2.2.5. Security Information

The Security Information field of the ATN Security Label shall be used to convey, as separate Tag Sets:

1. The Traffic Type and Routing Policy Requirements, if any, applicable to the transfer of the user data through the ATN.
2. The Security Classification

When no traffic type is identified then General Communications shall be assumed, with a routing policy requirement of "no preference". When no classification is specified then "unclassified" shall be assumed.

6.2.2.5.1 Encoding of the Security Information Field

The Security Information Field shall comprise zero, one or more Security Tag sets. A Security Tag with the same Tag Set Name shall not occur more than once.

Each Security Tag set shall consist of four fields, as illustrated in Figure 6-2, and defined below:

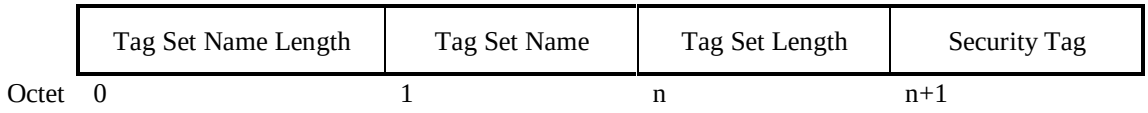


Figure 6-2: Security Tag Set Format

Note.— This format has been chosen to provide for an extensible type-length-value encoding method for security related information placed in the CLNP Header under rules specified by the ATN Security Authority.

6.2.2.5.2 Security Classification Registered Field Set

The Security Tag Set Name Length shall contain the length in octets of the Tag Set Name field

6.2.2.5.3 Security Tag Set Name

The Security Tag Set Name shall be used to uniquely identify the tag set.

6.2.2.5.4 Tag Set Length

The Tag Set Length Field shall contain the length in octets of the Security Tag field

6.2.2.5.5 Security Tag

The Security Tag field shall be used to convey security related information for which the syntax and semantics are identified by the preceding Tag Set Name.

6.2.2.5.6 Encoding of the Tag Set for Traffic Type and Associated Routing Policies

The Tag Set Name shall be set to [0000 1111]. When present in the Security Parameter, this tag set shall always be the first tag set to be encoded in the field.

Note.— This Tag Set is used to identify the traffic type of the data, whether it is for ATC or airline communications, and, for operational communications, any routing policy requirements that apply.

The Security Tag shall indicate the Routing Policy Requirements for the data contained in the same NPDU, according to Table 6-1.

Traffic Type	Category	Security Tag Value	Semantics
ATN Operational Communications	Air Traffic Service Communications (ATSC)	000 00001	No Traffic Type Policy Preference
		000 10000	Traffic only follows Class A ATSC route(s).
		000 10001	Traffic only follows Class B ATSC route(s).
		000 10010	Traffic only follows Class C ATSC route(s).
		000 10011	Traffic only follows Class D ATSC route(s).
		000 10100	Traffic only follows Class E ATSC route(s).
		000 10101	Traffic only follows Class F ATSC route(s).
		000 10110	Traffic only follows Class G ATSC route(s).
		000 10111	Traffic only follows Class H ATSC route(s).
		000 00011	Route Traffic using an ordered preference of Mode S first, then VHF Data Link, then Satellite Data Link, then HF Data Link.
	Aeronautical Operational Control (AOC)	001 00001	No Traffic Type Policy Preference.
		001 00010	Route Traffic only via Gatelink.
		001 00011	Route Traffic only via VHF Data Link.
		001 00100	Route Traffic only via Satellite Data Link.
		001 00101	Route Traffic only via HF Data Link.
		001 00110	Route Traffic only via Mode S Data Link.
		001 00111	Route Traffic using an ordered preference of Gatelink first, then VHF Data Link.
		001 01000	Route Traffic using an ordered preference of Gatelink first, then VHF Data Link, then Satellite.
		001 01001	Route Traffic using an ordered preference of Gatelink first, then VHF Data Link, then HF Data Link, then Satellite Data Link.
ATN Administrative Communications		001 10000	
General Communications		N/A[1]	
ATN Systems Management Communications		011 00000	

Table 6-1:-Encoding of Traffic Type Security Tag

Note 1.—General Communications traffic does not require encoding of security parameters within created NPDUs.

6.2.2.5.7 ATSC Route Selection - Tie Breaking

For a given ATSC class of service, route selection shall be based upon the route's capability to meet or exceed the required level of service (e.g., if Class D is selected by the application, routes which provide Class A, B, C, or D service may be used). If multiple routes are available which meet or exceed the selected service, the route with the lowest relative cost shall be selected.

Note1.— For the CNS/ATM-1 Package, subnetworks may be allocated a service class and a relative cost on a local basis for local routing policy decisions only.

Note2.— Transit delay values allocated to each ATSC class of service are expected to be enforced only on the air/ground path selection for the CNS/ATM-1 package.

6.2.2.5.8 Encoding of the Tag Set for Security Classification

The Tag Set Name shall be set to [0000 0011]. When present in the security parameter, this tag set shall always follow the Tag Set for Traffic Type and Associated Routing Policies (see 6.2.2.5) if present, but otherwise shall be the first tag set to be encoded in the field.

Note.— The purpose of this field is to permit the later extension of the ATN to handle classified data.

The Security Tag shall indicate the security classification of the NPDU. according to the following table:

Value	Security Classification
0000 0001	unclassified
0000 0010	restricted
0000 0011	confidential
0000 0100	secret
0000 0101	top secret
0000 0110 to 1111 1111	unassigned

6.2.3. Management of Network Priority

Note.— Network priority handling provisions are specified in Chapter 2.

6.2.4. Congestion Management

Note.— The congestion management provisions in the network layer are intended to guarantee the notification to the transport layer of potential risks of congestion via the C/E bit conveyed in QOS Maintenance parameter. The transport layer will take measures to avoid congestion if a high proportion of NPDUs are received with C/E bit set.

6.2.4.1. Setting of the congestion experienced flag

1. The *congestion experienced* flag in the QoS maintenance parameter in the options part of an NPDU header shall initially be set to zero by the originator of the NPDU.
2. When a NPDU is being forwarded by an ATN IS, the IS shall examine the depth of the output queue selected for that NPDU. If the depth of the selected output queue exceeds a threshold α, the ATN IS shall set the *congestion experienced* flag in the QoS maintenance parameter in the options part of the NPDU header.
3. Once the *congestion experienced* flag in the QoS maintenance parameter in the options part of an NPDU header is set, it shall not be reset by any ATN IS traversed by the NPDU further along to the path towards the destination.
4. When a destination network entity receives an NPDU of which the *congestion experienced* flag is set in the QoS maintenance parameter in the options part of the header of the NPDU, it shall convey the congestion experienced information to the destination transport entity by local means.

6.2.4.2. Required algorithm values

The value settings defined in the following table shall be implemented:

Name	Description	Required range
α	Output queue threshold	> 0 % and ≤ 10%

6.3. Compliance Statement

All Network entities shall implement ISO 8473 CLNP protocol and comply with all mandatory and optional internetwork protocol functions as specified in this chapter.

6.3.1. Mandatory Internetwork Protocol Functions

Note.— This section specifies the functions which are performed as part of the ATN Internetwork Protocol within all Network entities conforming to ATN requirements

6.3.1.1. PDU Composition Function

ATN ESs and ISs shall perform the PDU COMPOSITION function.

6.3.1.2. PDU Decomposition Function

ATN ESs and ISs shall perform the PDU DECOMPOSITION function.

6.3.1.3. Header Format Analysis Function

ATN ESs and ISs shall perform the HEADER FORMAT ANALYSIS function.

6.3.1.4. Route PDU Function

ATN ESs and ISs shall perform the ROUTE PDU function.

6.3.1.5. Forward PDU Function

ATN ESs and ISs shall perform the FORWARD PDU function.

6.3.1.6. Segmentation Function

ATN intermediate-systems (ISs) shall support both the segmenting and the non-segmenting subsets of ISO 8473. ATN ESs shall support ~~only~~ the ISO 8473 segmenting subset.

Recommendation. — *ATN ESs should use the non-segmenting ISO 8473 subset for NSDUs of up to 1024 octets.*

6.3.1.7. Reassembly Function

ATN ESs and ISs shall perform the REASSEMBLY function.

6.3.1.8. Discard PDU Function

ATN ESs and ISs shall perform the DISCARD PDU function.

6.3.1.9. Error Reporting Function

ATN ESs and ISs shall perform the ERROR REPORTING function.

6.3.1.10. PDU Header Error Detection

ATN ESs and ISs shall perform the PDU HEADER ERROR DETECTION function.

6.3.2. Optional Internetwork Protocol Functions

Note.— This section specifies the use of ISO CLNP optional functions within ATN ES and IS implementations.

ISO 8473 internetwork protocol options shall be selected by the ATN end-system Network entity which originates ISO 8473 NPDUs.

6.3.2.1. Padding Function

ESs shall not support the transmission of ISO 8473 NPDUs with the Padding Function. ISs shall support the transmission of NPDUs with the Padding Function. ESs and ISs shall support the receipt of ISO 8473 NPDUs with the Padding Function

6.3.2.2. Security Function

The SECURITY function shall be required for ATN ES or IS Network entity implementations receiving or transmitting traffic other than General Communications. ATN network entities shall therefore provide the Globally Unique Security format for all created NPDUs. The sole exception to this requirement is for General Communications traffic where no Security parameter information is required to be encoded in created NPDUs.

6.3.2.3. Source Routing Function

The SOURCE ROUTING function shall not be used by originating ATN ES Network entities. An ATN IS implementation shall process any NPDUs received with this option selected by discarding the NPDU. In the case that an NPDU is discarded, an ER NPDU shall be returned to the originating Network entity, if indicated by the Error Report flag in the discarded NPDU.

6.3.2.4. Record Route Function

ATN IS Network entities shall support the Partial RECORD ROUTE Function. ISs and ESs shall not support the Complete RECORD ROUTE Function.

6.3.2.5. Quality of Service Maintenance Function

ATN ES and IS Network entities shall support the Quality of Service Maintenance Function.

6.3.2.6. Priority Function

ATN ES and IS Network entities shall implement the PRIORITY Function.

6.3.2.7. Congestion Notification Function

ATN ES and IS Network entities shall support the Congestion Notification Function.

6.3.2.8. Echo Request Function

Recommendation. —— *ATN ES and IS Network entities should support the ECHO REQUEST Function as invoked by Network layer management.*

Note.— The Echo Request Function is invoked to obtain information on the reachability of specific network entities and the path characteristics between NEs through the operation of Network layer routing functions.

6.3.2.9. Echo Response Function

ATN ES and IS Network entities shall perform the ECHO RESPONSE Function upon receipt of an

Echo Request (ERQ) PDU that has reached its destination.

Note.— When invoked, this function causes an Echo Response (ERP) PDU to be created and processed by all ES and IS Network entities.

6.3.2.10. PDU Lifetime Control in Intermediate and End Systems

ATN ISs and ESs shall perform the PDU LIFETIME CONTROL function.

6.4. APRLs

Note.—The CLNP requirements list is a statement of which capabilities and options of the protocol at minimum are required to be implemented for the ATN environment. The requirements list may be used by the protocol implementor as a check list to conform to this standard; by the supplier and procurer to provide a detailed indication of the capabilities of an implementation; by the user to check the possibility of interworking between two different implementations; and by the protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance to the protocol.

6.4.1. Support of ATN-Specific Recommendations

Does the implementation support the following ATN-specific features:

Index	Item	SARPs Reference	CNS/ATM-1 Package Support
ATN CLNP1	Encoding and use of the Security Parameter	6.2.2	M
ATN CLNP2	Management of Network Priority	2.6	M

6.4.2. Major Capabilities

An ATN IS or ES protocol implementation shall conform to the following APRLs.

Item	Capability	Reference	Status	CNS/ATM-1 Package Support
ES	End System		O.1	O.1
IS	Intermediate System		O.1	O.1
FL-r	<r> Full protocol	6	M	M
FL-s	<s> Full protocol	6	M	M
NSS-r	<r> Non-segmenting subset	5.2	M	M
NSS-s	<s> Non segmenting subset	5.2	IS:M ^IS:O	IS:M ^IS:O~~X~~
IAS-r	<r> Inactive subset	5.2	ES:O	ES:O
IAS-s	<s> Inactive subset	5.2	IAS-r:M ^IAS-r:X	IAS-r:M ^IAS-r:X
S802	SNDCF for ISO 8802	8473-2 5.4	O.2	O
SCLL	SNDCF for CL Link Service	8473-4 5.3.1	O.2	O
SCOL	SNDCF for CO Link Service	8473-4 5.3.2	O.2	O
SX25	SNDCF for ISO 8208	8473-3 5.4	O.2	O
ATN SNDCF	SNDCF for Mobile Subnetworks	CNS/ATM-1 SARPs Ref: chapter 7	N/A	ISMOB:M ISGRD:O ^IS:O

ISMOB: If ISO 8473 is used over mobile subnetworks, then ISMOB is true, else ISMOB is false.

ISGRD: If ISO 8473 is used over ground subnetworks, then ISGRD is true, else ISGRD is false.

O.1: The supported functions, NPDUs, associated parameters and timers required for ESs are provided in APRLs 6.4.3 through 6.4.10. The supported functions, NPDUs, associated parameters and timers required for ISs are provided in APRLs 6.4.11 through 6.4.23.

O.2: APRLs for the SNDCF for use with ISO 8802-2 subnetworks are provided in 6.4.18 and 6.4.19. APRLs for the SNDCF for use with ISO 8208 subnetworks are provided in 6.4.20 through 6.4.23.

6.4.3. End Systems - Supported Functions

An ATN ES protocol implementation shall conform to the following APRL for supported functions.

Item	Function	Reference	Status	CNS/ATM-1 Package Support
ePDUC	PDU Composition	6.1	M	M
ePDUD	PDU Decomposition	6.2	M	M
eHFA	Header Format Analysis	6.3	M	M
ePDUL-s	<s> PDU Lifetime Control	6.4, CNS/ATM-1 SARPs Ref. 6.3.2.10	M	M
ePDUL-r	<r> PDU Lifetime Control	6.4, CNS/ATM-1 SARPs Ref. 6.3.2.10	O	M
eRout	Route PDU	6.5	M	M
eForw	Forward PDU	6.6	M	M
eSegm	Segment PDU	6.7	M	M
eReas	Reassemble PDU	6.8	M	M
eDisc	Discard PDU	6.9	M	M
eErep	Error Reporting	6.10	M	M
eEdec-s	<s> Header Error Detection	6.11	M	M
eEdec-r	<r> Header Error Detection	6.11	M	M
eSecu-s	<s> Security	6.13, CNS/ATM-1 SARPs Ref: 6.2.2	O	M
eSecu-r	<r> Security	6.13, CNS/ATM-1 SARPs Ref: 6.2.2	O	M
eCRR-s	<s> Complete Route Recording	6.15	O	OX
eCRR-r	<r> Complete Route Recording	6.15	O	O
ePRR-s	<s> Partial Route Recording	6.15	O	M
ePRR-r	<r> Partial Route Recording	6.15	O	M
eCSR	Complete Source Routing	6.14, CNS/ATM-1 SARPs Ref. 6.3.2.3	O	OX
ePSR	Partial Source Routing	6.14, CNS/ATM-1 SARPs Ref. 6.3.2.3	O	OX
ePRI-s	<s> Priority	6.17, CNS/ATM-1 SARPs Ref. 6.3.2.6	O	M

ePRI-r	<r> Priority	6.17, CNS/ATM-1 SARPs Ref. 6.3.2.6	O	M

Item	Function	Reference	Status	CNS/ATM-1 Package Support
eQOSM-s	<s> QOS Maintenance	6.16, CNS/ATM-1 SARPs Ref. 6.3.2.5	O	M
eQOSM-r	<r> QOS Maintenance	6.16, CNS/ATM-1 SARPs Ref. 6.3.2.5	O	M
eCong-s	<s> Congestion Notification	6.18	eQOSM-s:M	eQOSM-s:M
eCong-r	<r> Congestion Notification	6.18	O	M
ePadd-s	<s> Padding	CNS/ATM-1 SARPs Ref. 6.3.2.1	O	OX
ePadd-r	<r> Padding	CNS/ATM-1 SARPs Ref. 6.3.2.1	M	M
eEreq	Echo request	6.19	O	O
eErsp	Echo response	6.20	O	M
eSegS	Create segments smaller than necessary	6.8	O	O

6.4.4. End Systems - Supported NPDUs

An ATN ES protocol implementation shall conform to the following APRL for supported NPDUs.

Item	NPDU	Reference	Status	CNS/ATM-1 Package Support
eDT-t	DT (full protocol) transmit	7.7	M	M
eDT-r	DT (full protocol) receive	7.7	M	M
eDTNS-t	DT (non-segment) transmit	7.7	NSS-s:M	NSS-s:M
eDTNS-r	DT (non-segment) receive	7.7	M	M
eER-t	ER transmit	7.9	M	M
eER-r	ER receive	7.9	M	M
eIN-t	Inactive PDU transmit	7.8	IAS-s:M	IAS-s:M
[type REQ]eIN-r	Inactive PDU receive	7.8	IAS-r:M	IAS-r:M
eERQ-t	ERQ transmit	7.10	eEerq:M	eEreq:M
eERQ-r	ERQ receive	7.10	M	M
eERP-t	ERP transmit	7.11	eErsp:M	eErsp:M
eERP-r	ERP receive	7.11	M	M

6.4.5. End Systems - Supported DT Parameters

An ATN ES protocol implementation shall conform to the following APRL for supported DT parameters.

Item	Parameter	Reference	Status	CNS/ATM-1 Package Support
edFxPt-s	<s> Fixed Part	7.2	M	M
edFxPt-r	<r> Fixed Part	7.2	M	M
edAddr-s	<s> Address	7.3	M	M
edAddr-r	<r> Address	7.3	M	M
edSeg-s	<s> Segmentation Part	7.4	M	M
edSeg-r	<r> Segmentation Part	7.4	M	M
edPadd-s	<s> Padding	7.5.2	ePadd-s:M	-
edPadd-r	<r> Padding	7.5.2	M	M
edSecu-s	<s> Security	7.5.3	eSecu-s:M	eSecu-s:M
edSecu-r	<r> Security	7.5.3	eSecu-r:M	eSecu-r:M
edCRR-s	<s> Complete Route Recording	7.5.5	eCRR-s:M	-
edCRR-r	<r> Complete Route Recording	7.5.5	eCRR-r:M	eCRR-r:M
edPRR-s	<s> Partial Route Recording	7.5.5	ePRR-s:M	ePRR-s:M
edPRR-r	<r> Partial Route Recording	7.5.5	ePRR-r:M	ePRR-r:M
edCSR-s	<s> Complete Source Routing	7.5.4	eCSR:M	-
edPSR-s	<s> Partial Source Routing	7.5.4	ePSR:M	-
edQOSM-s	<s> QOS Maintenance	7.5.6	eQOSM-s or eCong-s:M	eQOSM:M
edQOSM-r	<r> QOS Maintenance	7.5.6	eQOSM-r or eCong-r :M	eQOSM or eCong-r:M
edPri-s	<s> Priority	7.5.7	ePRI-s:M	ePRI-s:M
edPri-r	<r> Priority	7.5.7	ePRI-r:M	eP-r:M
edData-s	<s> Data	7.6	M	M
edData-r	<r> Data	7.6	M	M
edUnSup2	Are received PDUs containing parameters selecting unsupported type 2 functions discarded and where appropriate an Error Report PDU generated ?	6.21	M	M
edUnSup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.21	M	M

6.4.6. End Systems - Supported ER Parameters

An ATN ES protocol implementation shall conform to the following APRL for supported ER parameters.

Item	Parameter	Reference	Status	CNS/ATM-1 Package Support
eeFxPt-s	<s> Fixed Part	7.2	M	M
eeFxPt-r	<r> Fixed Part	7.2	M	M
eeAddr-s	<s> Address	7.3	M	M
eeAddr-r	<r> Address	7.3	M	M
eePadd-s	<s> Padding	7.5.2	ePadd-s:M	-
eePadd-r	<r> Padding	7.5.2	M	M
eeSecu-s	<s> Security	7.5.3	eSecu-s:M	eSecu-s:M
eeSecu-r	<r> Security	7.5.3	eSecu-r:M	eSecu-r:M
eeCRR-s	<s> Complete Route Recording	7.5.5	eCRR-s:M	-
eeCRR-r	<r> Complete Route Recording	7.5.5	eCRR-r:M	eCRR-r:M
[type REQ]eePRR-s	<s> Partial Route Recording	7.5.5	ePRR-s:M	ePRR-s:M
eePRR-r	<r> Partial Route Recording	7.5.5	ePRR-r:M	ePRR-r:M
eeCSR-s	<s> Complete Source Routing	7.5.4	eCSR:M	-
eePSR-s	<s> Partial Source Routing	7.5.4	ePSR:M	-
eeQOSM-s	<s> QOS Maintenance	7.5.6	eQOSM-s or eCong-s:M	eQOSM-s or eCong-s:M
eeQOSM-r	<r> QOS Maintenance	7.5.6	eQOSM-r or eCong-r:M	eQOSM-r or eCong-r:M
eePri-s	<s> Priority	7.5.7	ePri-s:M	ePri-s:M
eePri-r	<r> Priority	7.5.7	ePri-r:M	ePri-r:M
eeDisc-s	<s> Reason for discard	7.9.5	M	M
eeDisc-r	<r> Reason for discard	7.9.5	M	M
eeData-s	<s> Data	7.9.6	M	M
eeData-r	<r> Data	7.9.6	M	M
eeUnSup2	Are received PDUs containing parameters selecting unsupported type 2 functions discarded and where appropriate an Error Report PDU generated ?	6.21	M	M
eeUnSup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.21	M	M

6.4.7. End Systems - Inactive DT Parameters

An ATN ES protocol implementation shall conform to the following APRL for inactive DT parameters.

Item	Parameter	Reference	Status	CNS/ATM-1 Package Support
eiNLPI-s	<s> Inactive Network Layer Protocol identifier	7.8.2	IAS-s:M	IAS-s:M
eiNLPI-r	<r> Inactive Network Layer Protocol Identifier	7.8.2	IAS-r:M	IAS-r:M
eiData-s	<s> Data	7.8.3	IAS-s:M	IAS-s:M
eiData-r	<r> Data	7.8.3	IAS-r:M	IAS-r:M

6.4.8. End Systems - Supported ERQ Parameters

An ATN ES protocol implementation shall conform to the following APRL for supported ERQ parameters.

Item	Parameter	Reference	Status	CNS/ATM-1 Package Support
eqFxPt-s	<s> Fixed Part	7.2	M	M
eqFxPt-r	<r> Fixed Part	7.2	M	M
eqAddr-s	<s> Address	7.3	M	M
eqAddr-r	<r> Address	7.3	M	M
eqSeg-s	<s> Segmentation Part	7.4	M	M
eqSeg-r	<r> Segmentation Part	7.4	M	M
eqPadd-s	<s> Padding	7.5.2	ePadd-s:M	-
eqPadd-r	<r> Padding	7.5.2	M	M
eqSecu-s	<s> Security	7.5.3	eSecu-s:M	eSecu-s:M
eqSecu-r	<r> Security	7.5.3	eSecu-r:M	eSecu-r:M
eqCRR-s	<s> Complete Route Recording	7.5.5	eCRR-s:M	-
eqCRR-r	<r> Complete Route Recording	7.5.5	eCRR-r:M	eCRR-r:M
eqPRR-s	<s> Partial Route Recording	7.5.5	ePr-s:M	ePrr-s:M
eqPRR-r	<r> Partial Route Recording	7.5.5	ePr-r:M	ePrr-r:M
eqCSR-s	<s> Complete Source Routing	7.5.4	eCSR:M	-
eqPSR-s	<s> Partial Source Routing	7.5.4	ePSR:M	-
eqQOSM-s	<s> QOS Maintenance	7.5.6	eQOSM-s or eCong-s:M	eQOSM:M
eqQOSM-r	<r> QOS Maintenance	7.5.6	eQOSM-r or eCong-r :M	eQOSM or eCong-r:M
eqPri-s	<s> Priority	7.5.7	ePri-s:M	ePri-s:M
eqPri-r	<r> Priority	7.5.7	ePri-r:M	ePri-r:M
eqData-s	<s> Data	7.6	M	M
eqData-r	<r> Data	7.6	M	M
eqUnSup2	Are received PDUs containing parameters selecting unsupported type 2 functions discarded and where appropriate an Error Report PDU generated ?	6.21	M	M
eqUnSup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.21	M	M

6.4.9. End Systems - Supported ERP Parameters

An ATN ES protocol implementation shall conform to the following APRL for supported ERP parameters.

Item	Parameter	Reference	Status	CNS/ATM-1 Package Support
epFxPt-s	<s> Fixed Part	7.2	M	M
epFxPt-r	<r> Fixed Part	7.2	M	M
epAddr-s	<s> Address	7.3	M	M
epAddr-r	<r> Address	7.3	M	M
epSeg-s	<s> Segmentation Part	7.4	M	M
epSeg-r	<r> Segmentation Part	7.4	M	M
epPadd-s	<s> Padding	7.5.2	ePadd-s:M	-
epPadd-r	<r> Padding	7.5.2	M	M
epSecu-s	<s> Security	7.5.3	eSecu-s:M	eSecu-s:M
epSecu-r	<r> Security	7.5.3	eSecu-r:M	eSecu-r:M
epCRR-s	<s> Complete Route Recording	7.5.5	eCRR-s:M	-
epCRR-r	<r> Complete Route Recording	7.5.5	eCRR-r:M	eCRR-r:M
epPRR-s	<s> Partial Route Recording	7.5.5	ePr-s:M	ePrr-s:M
epPRR-r	<r> Partial Route Recording	7.5.5	ePr-r:M	ePrr-r:M
epCSR-s	<s> Complete Source Routing	7.5.4	eCSR:M	-
epPSR-s	<s> Partial Source Routing	7.5.4	ePSR:M	-
epQOSM-s	<s> QOS Maintenance	7.5.6	eQOSM-s or eCong-s:M	eQOSM:M
epQOSM-r	<r> QOS Maintenance	7.5.6	eQOSM-r or eCong-r :M	eQOSM or eCong-r:M
epPri-s	<s> Priority	7.5.7	ePri-s:M	ePri-s:M
epPri-r	<r> Priority	7.5.7	ePri-r:M	ePri-r:M
epData-s	<s> Data	7.6	M	M
epData-r	<r> Data	7.6	M	M
epUnSup2	Are received PDUs containing parameters selecting unsupported type 2 functions discarded and where appropriate an Error Report PDU generated ?	6.21	M	M
epUnSup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.21	M	M

6.4.10. End Systems - Timers

An ATN ES protocol implementation shall conform to the following APRL for timers.

Item	Timer	Ref	ISO Status	ISO Range	CNS/ATM-1 Package Support	Values Supported
ELifReas	Is reassembly timer <= received derived PDU lifetime?	6.8	M		M	
eReasTim	Reassembly Timer	6.8		500ms to 127.5s		<= lifetime

6.4.11. Intermediate Systems - Supported Functions

An ATN IS protocol implementation shall conform to the following APRL for supported functions.

Item	Function	Reference	Status	CNS/ATM-1 Package Support
iPDUC	PDU Composition	6.1	M	M
iPDUD	PDU Decomposition	6.2	M	M
iHFA	Header Format Analysis	6.3	M	M
iPDUL	<s> PDU Lifetime Control	6.4	M	M
iRout	Route PDU	6.5	M	M
iForw	Forward PDU	6.6	M	M
iSegm	Segment PDU	6.7	iDSNS:M	iDSNS:M
iReas	Reassemble PDU	6.8	O	O
iDisc	Discard PDU	6.9	M	M
iErep	Error Reporting	6.10	M	M
iEdec	<s> Header Error Detection	6.11	M	M
iSecu	<s>Security	6.13 CNS/ATM-1 SARPs Ref: 6.2.2	O	M
iCRR	<s> Complete Route Recording	CNS/ATM-1 SARPs Ref. A9.3.2.4	O	OX
iPRR	<s> Partial Route Recording	6.15, CNS/ATM-1 SARPs Ref:6.3.2.4	O	M
iCSR	Complete Source Routing	CNS/ATM-1 SARPs Ref. 6.3.2.3	O	OX
iPSR	Partial Source Routing	6.14	O	OX
iPri	<s> Priority	6.17, CNS/ATM-1 SARPs Ref: 6.3.2.6	O	M
iQOSM	<s> QOS Maintenance	6.16, CNS/ATM-1 SARPs Ref: 6.3.2.5	O	M
iCong	<s> Congestion Notification	6.18, CNS/ATM-1 SARPs Ref: 6.3.2.7	O	M
iPadd	<s> Padding	6.12	M	M
iEreq	Echo request	6.19	O	O
iErsp	Echo response	6.20	O	M
iSegS	Create segments smaller than necessary	6.8	O	O
iDSNS	Simultaneous support of subnetworks with different SN-User data sizes	6.7	O	O

6.4.11.1. Supported Security Parameters

An ATN IS protocol implementation shall conform to the following APRL for supported security parameters.

Item	Function	Reference	Status	CNS/ATM-1 Package Support
iSADSSEC	Source Address Specific Security	7.5.3.1	iSecu:O.5	iSecu:O
iDADSSEC	Destination Address Specific Security	7.5.3.2	iSecu:O.5	iSecu:O
iGUNSEC	Globally Unique Security	CNS/ATM-1 SARPs Ref. 6.2.2	iSecu:O.5	iSecu:M

O.5: The Security parameter within a single NPDU specifies a security format code indicating Source Address Specific, Destination Address Specific or Globally Unique Security.

6.4.11.2. Quality of Service Maintenance Function

An ATN IS protocol implementation shall conform to the following APRL for the Quality of Service Maintenance function.

Item	Function	Reference	Status	CNS/ATM-1 Package Support
iQOSNAVAIL	If requested QOS not available, deliver at different QOS	6.16	iQOSM:M	iQOSM:M
iQOSNOT	Notification of failure to meet requested QOS	6.16	iQOSM:O	iQOSM:M
	Which of the following formats of QOS are implemented ?			
iSADDQoS	Source Address Specific QoS	7.5.6.1	iQoSM:O.3	iQOSM:O
iDADDQoS	Destination Address Specific QoS	7.5.6.2	iQoSM:O.3	iQOSM:O
iGUNQoS	Globally Unique QoS	7.5.6.3	iQoSM:O.3	iQOSM:M
iSvTD	Sequencing versus Transit Delay	7.5.6.3	iGUNQoS:O.4	iGUNQoS:O.4
iCongE	Congestion Experienced	7.5.6.3	iGUNQoS:O.4	iGUNQoS:M
iTDvCst	Transit Delay versus Cost	7.5.6.3	iGUNQoS:O.4	iGUNQoS:O.4
iREPvTD	Residual Error Probability versus Transit Delay	7.5.6.3	iGUNQoS:O.4	iGUNQoS:O.4
iREPvCst	Residual Error Probality versus Cost	7.5.6.3	iGUNQoS:O.4	iGUNQoS:O.4

O.3: The Quality of Service Maintenance parameter within a single NPDU specifies a QoS format code indicating Source Address Specific, Destination Address Specific or Globally Unique QoS.

O.4: If the QOS format code indicates that the Globally Unique QoS maintenance function is employed, then each bit in the associated parameter value may be set to indicate the order of intra and inter domain routing decisions based on QoS. The parameter values which apply to inter-domain routing are provided in Table 4 of ISO/IEC 10747.

6.4.12. Intermediate Systems - Supported NPDUs

An ATN IS protocol implementation shall conform to the following APRL for supported NPDUs.

Item	Function	Reference	Status	CNS/ATM-1 Package Support
iDT-t	DT (full protocol) transmit	7.7	M	M
iDT-r	DT (full protocol) receive	7.7	M	M
iDTNS-t	DT (non-segment) transmit	7.7	M	M
iDTNS-r	DT (non-segment) receive	7.7	M	M
iER-t	ER transmit	7.9	M	M
iER-r	ER receive	7.9	M	M
iERQ-t	ERQ transmit	7.10	iEreq:M	O
iERQ-r	ERQ receive	7.10	M	M
iERP-t	ERP transmit	7.11	iErsp:M	O
iERP-r	ERP receive	7.11	M	M

6.4.13. Intermediate Systems - Supported DT Parameters

An ATN IS protocol implementation shall conform to the following APRL for supported DT parameters.

Item	Parameter	Reference	Status	CNS/ATM-1 Package Support
idFxPt-s	<s> Fixed Part	7.2	M	M
idFxPt-r	<r> Fixed Part	7.2	M	M
idAddr-s	<s> Addresses	7.3	M	M
idAddr-r	<r> Addresses	7.3	M	M
idSeg-s	<s> Segmentation Part	7.4	M	M
idSeg-r	<r> Segmentation Part	7.4	M	M
idPadd-s	<s> Padding	7.5.2	M	M
idPadd-r	<r> Padding	7.5.2	M	M
idSecu-s	<s> Security	7.5.3	iSecu:M	iSecu:M
idSecu-r	<r> Security	7.5.3	iSecu:M	iSecu:M
idCRR-s	<s> Complete Route Recording	7.5.5	iCRR:M	M
idCRR-r	<r> Complete Route Recording	7.5.5	iCRR:M	-
idPRR-s	<s> Partial Route Recording	7.5.5	M	M
idPRR-r	<r> Partial Route Recording	7.5.5	iPRR:M	iPRR:M
idCSR-s	<s> Complete Source Routing	7.5.4	iCSR:M	-
idCSR-r	<r> Complete Source Routing	7.5.4	iCSR:M	-
idPSR-s	<s> Partial Source Routing	7.5.4	M	M
idPSR-r	<r> Partial Source Routing	7.5.4	iPSR:M	-
idQOSM-s	<s> QOS Maintenance	7.5.6	M	M
idQOSM-r	<r> QOS Maintenance	7.5.6	iQOSM or iCong:M	iQOSM or iCong:M
idPri-s	<s> Priority	7.5.7	M	M
idPri-r	<r> Priority	7.5.7	iPRi:M	iPri:M
idData-s	<s> Data	7.6	M	M
idData-r	<r> Data	7.6	M	M
idUnSup2	Are received PDUs containing parameters selecting unsupported type 2 functions discarded and where appropriate an Error Report PDU generated ?	6.19	M	M
idUnSup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.19	M	M

6.4.14. Intermediate Systems - Supported ER Parameters

An ATN IS protocol implementation shall conform to the following APRL for supported ER parameters.

Item	Parameter	Reference	Status	CNS/ATM-1 Package Support
ieFxPt-s	<s> Fixed Part	7.2	M	M
ieFxPt-r	<r> Fixed Part	7.2	M	M
ieAddr-s	<s> Address	7.3	M	M
ieAddr-r	<r> Address	7.3	M	M
ieSeg-s	<s> Seg Part	7.4	M	M
ieSeg-r	<r> Seg Part	7.4	M	M
iePadd-s	<s> Padding	7.5.2	M	M
iePadd-r	<r> Padding	7.5.2	M	M
ieSecu-s	<s> Security	7.5.3	iSecu:M	iSecu:M
ieSecu-r	<r> Security	7.5.3	iSecu:M	iSecu:M
ieCRR-s	<s> Complete Route Recording	7.5.5	M	M
ieCRR-r	<r> Complete Route Recording	7.5.5	iCRR:M	-
iePRR-s	<s> Partial Route Recording	7.5.5	M	M
iePRR-r	<r> Partial Route Recording	7.5.5	iPRR:M	iPRR:M
ieCSR-s	<s> Complete Source Routing	7.5.4	iCSR:M	-
ieCSR-r	<r> Complete Source Routing	7.5.4	iCSR:M	-
iePSR-s	<s> Partial Source Routing	7.5.4	M	M
iePSR-r	<r> Partial Source Routing	7.5.4	iPSR:M	-
ieQOSM-s	<s> QOS Maintenance	7.5.6	M	M
ieQOSM-r	<r> QOS Maintenance	7.5.6	iQOSM or iCong:M	iQOSM or iCong:M
iePri-s	<s> Priority	7.5.7	M	M
iePri-r	<r> Priority	7.5.7	iPri:M	iPri:M
ieDisc-s	<s> Reason for Discard	7.9.5	M	M
ieDisc-r	<r> Reason for Discard	7.9.5	M	M
ieData-s	<s> Data	7.6	M	M
ieData-r	<r> Data	7.6	M	M
ieUnsup2	Are received PDUs containing parameters selecting unsupported type 2 functions discarded ?	6.21	M	M
ieUnsup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.21	M	M

6.4.15. Intermediate Systems - Supported ERQ Parameters

An ATN IS protocol implementation shall conform to the following APRL for supported ERQ parameters.

Item	Parameter	Reference	Status	CNS/ATM-1 Package Support
iqFxPt-s	<s> Fixed Part	7.2	M	M
iqFxPt-r	<r> Fixed Part	7.2	M	M
iqAddr-s	<s> Addresses	7.3	M	M
iqAddr-r	<r> Addresses	7.3	M	M
iqSeg-s	<s> Segmentation Part	7.4	M	M
iqSeg-r	<r> Segmentation Part	7.4	M	M
iqPadd-s	<s> Padding	7.5.2	M	M
iqPadd-r	<r> Padding	7.5.2	M	M
iqSecu-s	<s> Security	7.5.3	iSecu:M	iSecu:M
iqSecu-r	<r> Security	7.5.3	iSecu:M	iSecu:M
iqCRR-s	<s> Complete Route Recording	7.5.5	iCRR:M	M
iqCRR-r	<r> Complete Route Recording	7.5.5	iCRR:M	-
iqPRR-s	<s> Partial Route Recording	7.5.5	M	M
iqPRR-r	<r> Partial Route Recording	7.5.5	iPRR:M	iPRR:M
iqCSR-s	<s> Complete Source Routing	7.5.4	iCSR:M	-
iqCSR-r	<r> Complete Source Routing	7.5.4	iCSR:M	-
iqPSR-s	<s> Partial Source Routing	7.5.4	M	M
iqPSR-r	<r> Partial Source Routing	7.5.4	iPSR:M	-
iqQOSM-s	<s> QOS Maintenance	7.5.6	M	M
iqQOSM-r	<r> QOS Maintenance	7.5.6	iQOSM or iCong:M	iQOSM or ICong:M
iqPri-s	<s> Priority	7.5.7	M	M
iqPri-r	<r> Priority	7.5.7	iPRi:M	iPri:M
iqData-s	<s> Data	7.6	M	M
iqData-r	<r> Data	7.6	M	M
iqUnSup2	Are received PDUs containing parameters selecting unsupported type 2 functions discarded and where appropriate an Error Report PDU generated ?	6.19	M	M
iqUnSup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.19	M	M

6.4.16. Intermediate Systems - Supported ERP Parameters

An ATN IS protocol implementation shall conform to the following APRL for supported ERP parameters.

Item	Parameter	Reference	Status	CNS/ATM-1 Package Support
ipFxPt-s	<s> Fixed Part	7.2	M	M
ipFxPt-r	<r> Fixed Part	7.2	M	M
ipAddr-s	<s> Addresses	7.3	M	M
ipAddr-r	<r> Addresses	7.3	M	M
ipSeg-s	<s> Segmentation Part	7.4	M	M
ipSeg-r	<r> Segmentation Part	7.4	M	M
ipPadd-s	<s> Padding	7.5.2	M	M
ipPadd-r	<r> Padding	7.5.2	M	M
ipSecu-s	<s> Security	7.5.3	iSecu:M	iSecu:M
ipSecu-r	<r> Security	7.5.3	iSecu:M	iSecu:M
ipCRR-s	<s> Complete Route Recording	7.5.5	iCRR:M	M
ipCRR-r	<r> Complete Route Recording	7.5.5	iCRR:M	-
ipPRR-s	<s> Partial Route Recording	7.5.5	M	M
ipPRR-r	<r> Partial Route Recording	7.5.5	iPRR:M	iPRR:M
ipCSR-s	<s> Complete Source Routing	7.5.4	iCSR:M	-
ipCSR-r	<r> Complete Source Routing	7.5.4	iCSR:M	-
ipPSR-s	<s> Partial Source Routing	7.5.4	M	M
ipPSR-r	<r> Partial Source Routing	7.5.4	iPSR:M	-
ipQOSM-s	<s> QOS Maintenance	7.5.6	M	M
ipQOSM-r	<r> QOS Maintenance	7.5.6	iQOSM or iCong:M	iQOSM or ICong:M
ipPri-s	<s> Priority	7.5.7	M	M
ipPri-r	<r> Priority	7.5.7	iPRi:M	iPri:M
ipData-s	<s> Data	7.6	M	M
ipData-r	<r> Data	7.6	M	M
ipUnsup2	Are received PDUs containing parameters selecting unsupported type 2 functions discarded and where appropriate an Error Report PDU generated ?	6.19	M	M
ipUnsup3	Are parameters selecting unsupported Type 3 functions ignored ?	6.19	M	M

6.4.17. Intermediate Systems - Timer and Parameter Values

An ATN IS protocol implementation shall conform to the following APRL for timers.

Item	Timer	Reference	Status	CNS/ATM-1 Package Support
iReasTim	Reassembly Timer	6.8	iReas:M	M

6.4.18. Subnetwork Dependent Convergence Functions SNDCF for use with ISO 8802-2 Subnetworks - Functions

When ISO 8802-2 is used as a subnetwork to support ATN service, the following APRL shall apply.

Item	Function	ISO/IEC 8473-2 Reference	Status	CNS/ATM-1 Package Support
S802SNUD	Is subnetwork user data of at least 512 octets transferred transparently by the SNDCF ?	5.2	M	M
S802SNTD	Is Transit Delay determined by the SNDCF prior to the processing of User Data ?	5.2	M	M

6.4.19. Subnetwork Dependent Convergence Functions SNDCF for use with ISO 8802-2 Subnetworks - Multi Layer Dependencies

When ISO 8802-2 is used as a subnetwork to support ATN service, the following APRL shall apply.

Item	Dependency	ISO/IEC 8473-2 Reference	CNS/ATM-1 Package Support
S802SSg-r	<r> Maximum SN data unit size (RX)	5.2	>=512
S802SSg-s	<s> Maximum SN data unit size (TX)	5.2	>=512

6.4.20. Subnetwork Dependent Convergence Functions SNDCF for use with ISO 8208 Subnetworks - Functions

When ISO 8208 is used as a subnetwork to support ATN service, the following APRL shall apply.

Item	Function	ISO/IEC 8473-3 Reference	Status	CNS/ATM-1 Package Support
XSNUD	Is Subnetwork User Data of at least 512 octets transferred transparently by the SNDCF ?	5.2	M	M
XSNTD	Is Transit Delay determined by the SNDCF prior to the processing of user data ?	5.2	M	M
	Call Setup Considerations	5.31		
	Is a new call setup:			
XCalla	a. when no suitable call exists ?	5.3.1 a.	O.3	O.3
XCallb	b. when queue threshold reached ?	5.3.1 b.	O.3	O.3
XCallc	c. by systems management ?	5.3.1 c.	O.3	O.3
XCalld	d. when queue threshold reached and timer expires ?	5.3.4	O.3	O.3
XCalle	e. by other local means ?	5.3.1	O.3	O.3
	Call clearing considerations Are calls cleared:	5.3.2		
XClra	a. when idle timer expires	5.3.2 a.5.3.4	O	O
XClrb	b. when need to re-use circuit	5.3.2 b.	O	O
XClrc	c. by systems management	5.3.2 c.	O	O
XClrd	d. by provider ?	5.3.2 d.	M	M
XClrer	e. by other local means ?	5.3.2	O	O
XPD	X.25 Protocol Discrimination	5.3.3	M	M
XVCC	Resolution of VC collisions	5.3.5	M	M
XMCR	Multiple VCs responding	5.3.6	M	M
XMCI	Multiple VCs initiating	5.3.6	O	O
Xpri	X.25 Priority procedure	5.3.7	O	M

6.4.21. Subnetwork Dependent Convergence Functions SNDCF for use with ISO 8208 Subnetworks - X.25 Call User Data

When ISO 8208 is used as a subnetwork to support ATN service, the following APRL shall apply.

Item	Parameter	ISO/IEC 8473-3 Reference	Status	CNS/ATM-1 Package Support
PD-s	<s> Protocol Discriminator	5.3.3	M	M
PD-r	<r> Protocol Discriminator	5.3.3	M	M
LI-s	<s> Length Indication	5.3.6	XMCI:M	XMCI:M
LI-r	<r> Length Indication	5.3.6	M	M
Ver-s	<s> SNCR Version	5.3.6	XMCI:M	XMCI:M
Ver-r	<r> SNCR Version	5.3.6	M	M
SNCR-s	<s> SNCR Value	5.3.6	XMCI:M	XMCI:M
SNCR-r	<r> SNCR Value	5.3.6	M	M

6.4.22. Subnetwork Dependent Convergence Functions SNDCF for use with ISO 8208 Subnetworks - ISO 8208 SNDCF Timers

When ISO 8208 is used as a subnetwork to support ATN service, the following APRL shall apply.

Item	Timer	ISO/IEC 8473-3 Reference	Status	Values	CNS/ATM-1 Package Support
XIDL	X25 VC Idle	5.3.4	XClra:O	Any	~~M~~ XClra:O
XNVC	additional VC	5.3.4	O	Any	M

6.4.23. Subnetwork Dependent Convergence Functions SNDCF for use with ISO 8208 Subnetworks - SNDCF Multi Layer Dependencies

When ISO 8208 is used as a subnetwork to support ATN service, the following APRLs shall apply.

Item	Dependency	ISO/IEC 8473-3 Reference	CNS/ATM-1 Package Support	Values Supported
XSSg-r	<r> Maximum SN data unit size (Rx)	5.2	>=512	>=512
XSSg-s	<s> Maximum SN data unit size (Tx)	5.2	>=512	>=512

Item	Dependency	ISO/IEC 8473-3 Reference	Status	CNS/ATM-1 Package Support
Xvc	X.25 Virtual call service	5.3.8	M	M
Xdt	X.25 Data transfer	5.3.8	M	M
Xfc	X.25 flow control procedures	5.3.8	M	M
Xfrp	X.25 flow control + reset packets	5.3.8	M	M
Xccp	X.25 call setup and clear packets	5.3.8	M	M
Xdp	X.25 DTE and DCE data packets	5.3.8	M	M
Xrs	X.25 restart procedures	5.3.8	M	M
XDct	X.25 DCE timeouts	5.3.8	M	M
XDtT	X.25 time limits	5.3.8	M	M
Xpco	X.25 network packet coding	5.3.8	M	M
Xfcn	X.25 flow control parameter negotiation	5.3.8	O	O
Xtd	X.25 transit delay selection and negoiation	5.3.8	O	O
Xtc	X.25 throughput class negotiation	5.3.8	O	O
Xoth	Other X.25 elements	5.3.8	O	O

7. SPECIFICATION OF SUBNETWORK DEPENDANT CONVERGENCE FUNCTIONS

7.1. Scope and Applicability

The *Subnetwork Service* (SN-Service) as specified in this chapter shall be provided to the ISO 8473 Internetwork Protocol and the ISO 9542 End-System to Intermediate-System Protocol.

A *Subnetwork Dependent Convergence Function* (SNDCF) shall be provided where the available SNAcP does not provide the connectionless SN-Service assumed by the ATN Internet Protocols.

Note 1.— The ATN Internetwork layer, including CLNP and the routing protocols that support it, assume a common connectionless service to be provided by all subnetworks providing communications between ATN systems.

Note 2.— For the purposes of describing the notional interfaces between different OSI protocol layers, each protocol layer is assumed to provide a service to the next higher layer. The assumed service provided by the subnetworks is described in ISO 8473 clause 5.5 and 8.

Note 3.— There is no requirement to implement this service as a software interface.

.

7.2. Mobile Subnetwork routing initiation and termination

Note.— These procedures are defined in Chapter 3.

7.3. Subnetwork Service Primitives

The mechanisms defined in this chapter, or equivalent mechanisms shall be provided.

Table 7-1: SN-Service Primitives and Associated Parameters

Parameter	SN-UNITDATA Request	SN-UNITDATA Indication
SN-Source-Address	Mandatory	Mandatory
SN-Destination-Address	Mandatory	Mandatory
SN-Priority	Optional	Optional
SN-Quality-of-Service	Optional	Optional
SNS-Userdata	Mandatory	Mandatory

The service to support SN-Service-Users shall be defined by the primitives in Table 7-1. The SN-Source-Address, SN-Destination-Address and SNS-Userdata parameters shall be mandatory, while the SN-Priority and SN-Quality-of-Service parameter shall be optional.

7.3.1. Subnetwork Service primitives parameters

7.3.1.1. Subnetwork Point of Attachment (SNPA) Addresses

The SN-Source-Address and SN-Destination-Address parameters shall specify the points of attachment to a public or private subnetwork(s). The SN-Source-Address and SN-Destination-Address addresses shall include information denoting a particular underlying subnetwork, as well as addressing information for systems attached directly to that subnetwork.

SNPA values for a particular subnetwork shall be those specified and administered by the authority responsible for administration of that subnetwork.

7.3.1.2. Subnetwork Priority

If supported by the subnetwork, the SN-Priority, as specified in Table 7-1, parameter shall specify the relative importance of the associated SNS-Userdata parameter, and may influence the order in which the SNS-Userdata are transferred via the real underlying subnetwork service.

SN-Priority values shall be in the range **[0000 0000]** through **[0000 1110]**, with higher values indicating higher priorities. If no SN-Priority is indicated, the value **[0000 0000]** shall be assumed to be the default.

7.3.1.3. Subnetwork Quality of Service (SNQOS)

If supported, the SN-Quality-of-Service parameter shall comprise the following information:

1. Transit Delay;
2. Residual Error Probability;
3. Economic cost; and,
4. Protection against Unauthorized Access.

Use of the SN-Quality-of-Service parameter shall be optional, and shall be based on the needs of the SN-Service-User. If required by the SN-Service-User, the SN-Quality-of-Service parameter shall be used to influence the service requested from the Subnetwork Provider to support transfer of SN-UNITDATA requests. Techniques for mapping the semantic content of SN-Quality-of-Service parameter onto mechanisms provided for a particular underlying subnetwork shall be based on a priori information and local management options.

7.3.1.4. Subnetwork Service Userdata

The SNS-Userdata shall contain the ISO 8473 or ISO 9542 NPDU that have to be conveyed between adjacent network entities. The SNS-Userdata shall be an ordered multiple of octets, and shall be transferred transparently between the subnetwork points of attachment specified in the SNS primitive.

7.3.2. Subnetwork Service Data Units (SNSDUs)

ISO 8473 and ISO 9542 PDUs shall be conveyed between adjacent network entities as SNSDUs, through invocation of the SN-UNITDATA service with the ISO 8473 or ISO 9542 NPDU provided as the SNS-Userdata parameter. ~~The underlying subnetwork shall support a SDU size of a minimum of 1068 octets.~~

~~*Note. — The 1068 octet number is derived from a 1024 octet user data, 9 octet fixed ISO 8473 header, 42 octet Source and Destination NSAP Addresses, 6 octets for segmentation fields and 4 octets to support SNDCF local reference option.*~~

7.4. Subnetwork Dependent Convergence Function (SNDCF)

The SNDCF shall provide a connectionless-mode service in the case where an underlying subnetwork does not inherently provide the connectionless-mode service assumed by the SNS-User. If an underlying subnetwork inherently provides a connection-mode service, the SNDCF shall provide a mapping onto the underlying service.

7.5. Convergence Provisions for ISO 8208 Subnetworks

The facility provided for convergence of ISO 8473 and ISO 9542 over the ISO 8208 SNAcP shall establish, maintain and release ISO 8208 virtual circuits as needed, and shall provide for the priority and QOS requirements of ISO 8473 and ISO 9542. The interface between the SNDCF and the SN-Service-Users shall be the SN-UNITDATA request/indication primitives listed in Table 7-1.

7.5.1. Service Coordination between the SNDCF and SN-Service-Users

On receipt of a SN-UNITDATA request, the SNDCF shall either establish a new virtual circuit or make available an existing virtual circuit which meets the priority and QOS requirements of the SN-Service-User as specified by the SN-Priority and SN-Quality-of-Service parameters, if present. If the SN-Priority and SN-Quality-of-Service parameters are not present in a received SN-UNITDATA request, the SNDCF shall use local default parameter values; in this case, it shall be assumed that the SN-Service-User has accepted the default QOS available from the underlying subnetwork.

7.5.2. Service Coordination between the SNDCF and ISO 8208 Subnetwork Providers

If any combination of the Transit Delay Selection and Indication, Throughput Class Negotiation or Priority ISO 8208 optional user facilities are

available from the Subnetwork Provider via the Subnetwork Access Protocol, then the SNDCF shall use them for service coordination at the time of establishment of virtual circuits, as described in 7.5.2.1, 7.5.2.5 and 7.5.2.6. If one or more of these three ISO 8208 optional user facilities are not available from the Subnetwork Provider via the ISO 8208 Subnetwork Access Protocol, default values for transit delay, throughput class and priority shall be assumed by the SNDCF.

7.5.2.1. Transit Delay

The SNDCF shall invoke the Transit Delay Selection and Indication Facility, if provided, when:

1. A new virtual circuit must be established;
2. Transit Delay is indicated in the SN-UNITDATA request primitive causing establishment of the new virtual circuit; and,
3. Expected Transit Delay for the selected subnetwork is unknown.

If the requested maximum transit delay is less than the transit delay available from the Subnetwork Provider, the SNDCF shall attempt to transfer the SN-UNITDATA request at a greater transit delay than requested. If the indicated value is equal to or greater than the transit delay available from the Subnetwork Provider, the SNDCF shall transfer the SN-UNITDATA request. The requested maximum transfer delay shall apply to both directions of transfer.

7.5.2.1.1. Transit Delay Selection and Indication Facility

The SNDCF shall indicate the requested transit delay by means of the Transit Delay Selection and Indication Facility in the CALL REQUEST packet.

Recommendation.— *The Subnetwork Provider, when able to do so, should allocate resources and route the Virtual Circuit in a manner such that the transit delay applicable to that circuit does not exceed the desired transit delay.*

When the Transit Delay Selection and Indication Facility is invoked, the INCOMING CALL packet transmitted to the called SNDCF and the CALL CONNECTED packet transmitted to the calling SNDCF shall both contain the indication of the transit delay applicable to the Virtual Circuit.

7.5.2.2. Residual Error Probability

The SNDCF shall discard an SN-UNITDATA request primitive and its associated SN-Userdata parameter if the requested maximum residual error probability is less than the residual error probability known to be available from the Subnetwork Provider. If the requested value is equal to or greater than the residual error probability known to be available from the Subnetwork Provider, the SNDCF shall transfer the SN-UNITDATA request. The requested maximum residual error probability shall apply to both directions of transfer.

7.5.2.3. Economic cost

The SNDCF shall discard an SN-UNITDATA request primitive and its associated SN-Userdata parameter if the requested maximum economic cost is less than the economic cost known to be available from the Subnetwork Provider. If the requested value is equal to or greater than the economic cost known to be available from the Subnetwork Provider, the SNDCF shall transfer the SN-UNITDATA request. The requested maximum cost determinant shall apply to both directions of transfer.

7.5.2.4. Protection against Unauthorized Access

The Subnetwork Provider shall inform the SN-Service-User of the level of protection provided for data in transit. The level of protection shall be specified as one of the following four qualitative options:

1. No protection.
2. Protection against passive monitoring of SNSDU traffic flow.
3. Protection against active modification of SNSDU traffic flow.
4. Protection against both passive monitoring and active modification of SNSDU traffic flow.

If the SN-Service-User includes information in the SN-Quality-of-Service parameter indicating the required level of protection in the SN-UNITDATA request primitive and the Subnetwork Provider cannot satisfy this requirement, then the SNDCF shall discard the SN-UNITDATA request primitive and its associated SN-Userdata parameter.

7.5.2.5. Throughput

Subnetwork throughput shall be determined or negotiated in one of two ways:

1. Throughput information may be available as a priori information from the Subnetwork Provider; or,
2. Throughput information may be dynamically indicated and/or negotiated by the SNDCF, using the ISO 8208 Throughput Class Negotiation Facility.

Recommendation.— *If the throughput required by the SN-Service-User is greater than the throughput which can be provided, the SNDCF should opt for another Subnetwork Provider, if available.*

7.5.2.5.1. Throughput Class Negotiation Facility

Recommendation.— *The SNDCF should make use of the ISO 8208 Throughput Class Negotiation Facility for indication and/or negotiation of Throughput Class, if offered by the subnetwork service provider.*

If Throughput Class Negotiation is used by the SNDCF, the calling SNDCF shall request throughput classes for both directions of data transmission via the ISO 8208 Call Request packet.

The throughput class indicated to the called SNDCF shall not be greater than the default throughput classes, for each direction of transmission, at the calling and called SNDCF Subnetwork Provider interfaces respectively.

Note.— The supplied throughput may be less than indicated throughput.

7.5.2.6. Priority

The SNDCF shall have a priori information regarding the use of priority by the Subnetwork Provider.

If the Subnetwork Provider supports priority and specifies the mapping of Network Service to Subnetwork Service priorities:

1. The SNDCF shall convey the priority to the Subnetwork Provider by means of the ISO 8208 priority facility, as described in 7.5.2.6.1. If the subnetwork supports priority values ranging from **[0000 0000]** to **[0000 1110]**, the subnetwork priority value shall be the same as the priority value in the ISO 8473 or ISO 9542 header, respectively to provide a one-to-one mapping between the network and subnetwork layer priorities. If fewer (or more) than fourteen levels of subnetwork priority are supported, the priority value in the ISO 8473 or ISO 9542 header shall be mapped onto the subnetwork priority value according to the requirements of the subnetwork provider.
2. The SNDCF shall establish a SN-connection for each requested priority. A SN-connection shall only be used for SNSDUs for which the indicated priority corresponds with the priority associated with the connection.

If the Subnetwork Provider does not require connections to be prioritized, then the SNDCF shall not convey priority information to the Subnetwork Provider and the provisions of 7.5.2.6.1 and 7.5.2.6.2 shall not apply.

7.5.2.6.1. Use of the Priority Facility

If no SN-connection with the requested priority is available, the SNDCF shall establish a connection by sending a CALL REQUEST containing the appropriate priority facility to the Subnetwork Provider. Upon receipt of an INCOMING CALL packet from the Subnetwork Provider the called SNDCF shall map the contents of the priority parameter field into the priority parameter of the CALL ACCEPTED packet.

Note 1.— The Priority Option is mandatory within an ISO 8473 NPDU as specified in Chapter 6.

Note 2.— Neither the priority to gain a connection nor to keep a connection are specified.

7.5.3. Convergence Provisions for ISO 8208 General Topology Subnetworks

The subnetwork service specified in 7.1 shall be provided using ISO 8208 General Topology Subnetworks as specified in ISO 8473, and as qualified by 7.6.2.

Recommendation.— *All ATN ESs and ISs using ISO 8208 Fixed Subnetworks for communication with other ATN ESs and ISs should implement the SNDCF as specified in 7.6.4..*

7.5.4. Convergence Provisions for ISO 8208 Mobile Subnetworks

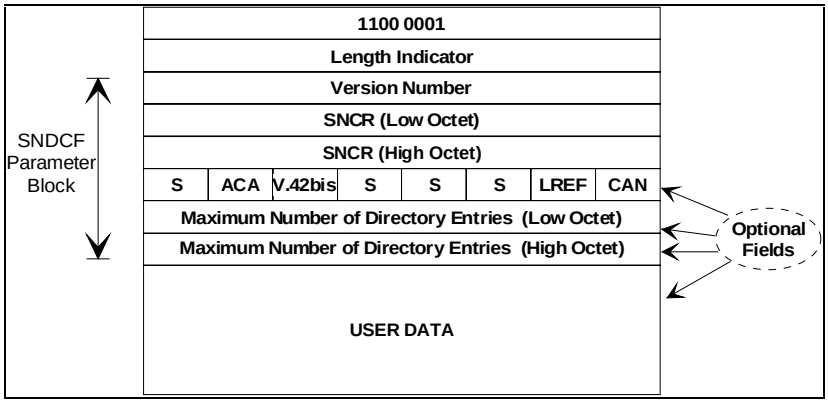
The subnetwork service specified in 7.1 shall be provided using the SNDCF for ISO 8208 Mobile Subnetworks as specified in this clause and its subordinate paragraphs, and as qualified by 7.5.2.

Note 1.— The SNDCF specified below is only applicable when providing the SN-UNITDATA service to ISO 8473, ISO 9542 and ISO/IEC 10589 network layer protocols. Unpredictable behavior may result if used to support other Network Layer Entities.

Note 2.— An optional feature of the SNDCF provides for "local reference cancellation"

Recommendation.— *Implementations using this SNDCF for air-ground communications should only implement the optional facility for local reference cancellation when the lifetime of the virtual circuits is of the same order as the flight time.*

Recommendation.— *Implementations using this SNDCF for ground/ground communications should use the optional local reference cancellation mechanism.*



F**igure 7.1**: Format for Call Request User Data

7.5.4.1. Scope and Applicability

The mobile SNDCF shall be used solely for the provision of the SN-UNITDATA service to ISO 8473, ISO 9542 and ISO/IEC 10589 network layer entities.

7.5.4.2. Conformance

All ATN ISs using mobile ISO 8208 subnetworks for communication with other ISs shall implement the SNDCF procedures and local reference header compression of the DT and Error PDU headers, as specified below.

7.5.4.3. Call Setup

On receipt of a SN-UNITDATA request or based on local system management action, and lacking a suitable existing virtual circuit, the SNDCF shall establish a new virtual circuit meeting the priority and QOS requirements expressed in the SN-UNITDATA request.

7.5.4.3.1. Call Setup Mechanism and Timing

The mechanism and timing for opening a virtual circuit to a known SNDCF prior to the transmission of SNSDUs shall be determined:

1. dynamically, or
2. by the explicit intervention of Systems Management, identifying the destination SNDCF's SNPA address,

7.5.4.3.2. Call Setup Functions

When it has been determined that a virtual circuit is to be made available, the calling SNDCF shall perform all functions associated with establishing a virtual circuit. The SNDCF shall send an ISO 8208 CALL REQUEST packet to the DTE Address specified as the SN-Destination-Address, with the following optional user facilities and CCITT-specified DTE facilities:

1. Priority shall be set if the subnetwork provider supports priority and specifies the mapping of Network Service to Subnetwork Service priorities. The priority value passed in the SN-UNITDATA request shall apply to priority of data on a connection. If the priority to gain a connection and/or priority to keep a connection is conveyed within the ISO 8208 Facility Parameter Field, these priorities shall be consistent with the priority of data on a connection.
2. Non-standard default packet size to the maximum supported by the subnetwork.
3. Fast Select shall be used if available.

Note 1.— Other optional user facilities and CCITT-specified DTE facilities may be required by subnetworks. The use of these facilities is a local matter.

Note 2.— The SNDCF is assumed to know, a priori, if a given subnetwork supports prioritization of virtual circuits, the number of discrete priority levels supported and the relationship between the subnetwork priority and SNSDU priority.

Note 3.— The mapping between SNSDU priority and subnetwork priority is specified separately for each subnetwork type.

Note 4.— If Fast Select is not supported, the compression algorithms cannot be negotiated.

7.5.4.3.3. Format of Call Request and Call Accept User Data

7.5.4.3.3.1. Call Request User Data

The call user data field layout shall be as illustrated in Figure 7.1. The field is variable in length, and shall be constructed as follows:

1. The first octet of the call user data field of the Call Request packet (the *Subsequent Protocol Identifier* (SPI)) shall be set to Binary 1100 0001 to indicate that the virtual circuit is to be used to provide the underlying service by this SNDCF.
2. The second octet is a length indicator giving the number of octets in the SNDCF parameter block (including this length indicator up to

and including (if present) the maximum number of directory entries field).

3. The third octet is the SNDCF version indicator and shall be set to 0000 0001 to indicate this version of the SNDCF protocol.

4. The fourth and fifth octets form the Subnetwork Connection Reference (SNCR) . The value encoded in this field shall be the number of virtual circuits currently established between the calling and called DTEs (i.e. the originating and the responding SNDCFs) at this call priority.

5. The sixth octet identifies the compression techniques supported by this ATN SNDCF. The bit fields in this octet indicates the following as shown in Figure 7.1.

Note 1.— Multiple compression techniques may be supported.

Stream Compression Options

bit 8:	Spare (S)
bit 7:	*ICAO Address Compression Algorithm (ACA)*
bit 6:	V.42 BIS
bit 5:	Spare (S)

Note 2 .— The use of the stream compression algorithms referenced above is subject to validation.

Dictionary Compression Options

bit 4:	Spare (S)
bit 3:	Spare
bit 2:	*Local Reference* (LREF) option
bit 1:	*Local Reference Cancellation Option* (CAN) supported

When bit 2 is set in the ISO 8208 Call Request, the LREF CLNP Header Compression is offered. Bit 1 may only be set if bit 2 is also set. When bit 2 is set the local reference cancellation procedures are also offered.

At most, one of the stream compression algorithms can be used, so bits 6 and 7 can both be offered in the call request packet, but both cannot be set in the call response packet.

6. When the LREF compression algorithm is used, i.e if bit 2 in octet six is set, the seventh and eight octet (Maximum Directory Entries) identifies the maximum number of directory entries supported for the local reference (minimum size 128), as an unsigned even number.

   When the LREF compression algorithm is not used, the seventh octet is the first octet of the additional Data field .

7. When the LREF option is used , the Additional User Data field starts at octet nine.

Note 6.— The Additional User Data field may be used to convey the ISO 9542 ISH PDU as part of the routing initiation sequence.

Note 7.— ISO TR 9577 provides the international register for SPI values. The value binary 1100 0001 has not been assigned by the ISO Technical Report and it is unlikely that it will be. However, it is not guaranteed to be unambiguous outside of the scope of the ATN.

7.5.4.3.3.2. Call Accept User Data

The call accept user data field layout shall be as illustrated in Figure 7.2. The field is variable in length, and shall be constructed as follows:

1. The first octet identifies the compression techniques supported by this ATN SNDCF. The bit fields has the same meaning as the one used for the sixth octet of the Call Request User Data (See Note 1 and 2 in the previous section)

2. The Second octet is the first octet of the Additional User Data field.

Note.— When the fast select facility is available, the Additional User Data field may be used to convey the ISO 9542 ISH PDU as part of the routing initiation sequence.

7.5.4.3.4. Application of Compression Procedures

The order in which compression algorithms and ISO 8208 segmentation are applied shall be as follow :

- If the LREF compression algorithm is used , it shall be applied to the ISO 8473 PDU first.
- If the stream compression algorithm is used , it shall be applied next.
- Finally, if the PDU is still large enough to need M-bit sequencing procedures, these shall then applied.

This sequence is inverted on the receiving end.

- If Re-segmentation is required , Re-segmentation based on the M-bit shall be done first.
- If a stream decompression algorithm is used it shall be applied next

- Finally if the LREF compression is used, the LREF decompression algorithm shall then be applied.

7.5.4.3.5. Call acceptance and compression negotiation

When a Call Indication is received, the called SNDCF first shall check for a call collision. If the SNDCF has an outstanding Call Request to the same DTE Address, as given as the calling DTE in this Call Indication, and the call priority and SNCR are identical, then a call collision has occurred, and the call collision resolution procedures specified in ISO 8473 Clause 8.4.3.5 shall be invoked to resolve the call collision.

Figure 7.2: Format for Call Accept User Data

The called SNDCF then performs those operations associated with accepting a call, provided that none of the reasons for rejection listed in 7.5.4.3.6 occurs, but generates no SN-UNITDATA indication; The priority on call acceptance shall be that proposed by the calling SNDCF.

If the call is acceptable then the Called SNDCF shall accept the call and indicate the combination of compression techniques acceptable to the SNDCF, out of those proposed by the Calling SNDCF, by including the one-octet field shown in Figure 7.2, in the ISO 8208 Call Accept User Data. The Called SNDCF shall indicate support for no more than one stream compression option.

If the called SNDCF accepts the call indicating that a proposed compression procedure is not supported, then the Calling SNDCF shall maintain the virtual circuit and shall not apply this compression procedure.

If the Called SNDCF accepts the call and if the Call User Data contains the User Data fields then the Called SNDCF shall process the PDU in the User Data field according to 7.5.4.7.

On receipt of User Data in the Call Accept User Data field, then the Calling SNDCF shall process the PDU in the User Data field according to 7.5.4.7.

7.5.4.3.6. Call rejection

If the call is not permitted by the effective security policy of the called SNDCF, then the call shall be rejected with a diagnostic code of 1000 0101 (see table 7-6). This call shall also be rejected for the following reasons :

- The proposed ISO-8208 facility, priority or fast select is not available
- Fast Select not supported and a proposed compression algorithm is not supported
- The format of the call user data is invalid
- The version number is not supported
- The Local reference compression is supported and the called SNDCF does not support the proposed directory size.

Recommendation. — *If a call is rejected due to the proposed directory size being too large, the caller should re-attempt the call using the default directory size, thus ensuring that the call will not be rejected again due to the requested directory size*

If the calling SNDCF receives a Clear Indication indicating call rejection, other than as part of a call collision resolution or directory size negotiation, then a Systems Management notification shall be generated, and any SN-UNITDATA queued for this call shall be discarded.

.

The diagnostic code listed in table 7-6 shall be used when an SNDCF rejects an incoming Call Request.

7.5.4.4. Local Directory Initialization

Both calling and called SNDCFs shall create a local directory to be associated with each newly established virtual circuit. This directory shall consist of entries numbered from zero to a maximum of 32767, each entry consisting of:

1. A pair of NSAP Addresses, known as the inward and outward NSAP Addresses respectively;
2. The ISO 8473 protocol version number
3. The value of the security options parameter (see ISO 8473 Clause 7.5.3), which may be empty;

The directory shall be initially empty. The mobile SNDCF shall support a minimum directory size of 128 entries.

7.5.4.5. Action following an SN-UNITDATA Request

On receipt of a SN-UNITDATA request the SNDCF shall identify an appropriate virtual circuit to the subnetwork user associated with the SN-

Destination-Address, and which satisfies the PDU priority and Security requirements, and queue the accompanying PDU (i.e. the user data associated with the SN-UNITDATA request) for transfer over that virtual circuit.

If there is no virtual circuit which satisfies the PDU priority and Security requirement, then the SNDCF shall try to establish a virtual circuit with adequate security and with the PDU priority.

If a suitable virtual circuit can be established, then the PDU shall then be queued for transfer over the newly established virtual circuit. If no such virtual circuit can be established, then if an existing virtual circuit associated with the SN-Destination-Address provides an adequate level of security and priority, the PDU shall be queued for transfer over the existing virtual circuit. Otherwise, the PDU shall be discarded.

Note 1.— The opening of an additional virtual circuit for this purpose may be inappropriate in certain cases. For example, opening an additional virtual circuit via a single frequency VDL subnetwork or via the Mode S subnetwork will not necessarily result in increased capacity.

Note 2.— The maintenance of the minimum QOS level includes ensuring that the number of local references that are required to support the number of data streams multiplexed over a given virtual circuit does not exceed the number available.

If no virtual circuit exists to the SN-Destination-Address, and the circuit is not classified as dynamically assigned by the IS-IS routing protocol or under a static routing regime, then the SN-UNITDATA shall be discarded, with an error report sent to a System Manager.

Note 3.— Virtual Circuits between ISs and between ISs and ESs are initially established by procedures associated with the specific routing procedures employed. If no such virtual circuit has been established, or may be established under the routing procedures, then no route exists and hence it is an error if an attempt is made to send a PDU over such a route.

7.5.4.5.1. Identification of Network Layer Protocol

Prior to transmission of an SN-UNITDATA SN-Userdata parameter over a virtual circuit, the SNDCF shall inspect the initial octet of the SN-Userdata parameter (*Initial Protocol Identifier* (IPI)) to identify the network layer protocol contained within the SN-UNITDATA request. If the IPI contains binary **[1000 0001]** indicating ISO 8473, then the procedures in 7.5.4.5.2 shall be performed.

If the IPI contains binary **[1000 0010]** indicating ISO 9542 (ES-IS), binary **[1000 0011]** indicating ISO/IEC 10589 (IS-IS), or binary **[0100 0101]** indicating ISO/IEC 11577 (NLSP), then the packet shall be sent unchanged over the virtual circuit, using the M-bit segmentation mechanism, if the packet is larger than the maximum length of user data permitted for the virtual circuit. If the IPI contains any other value the SN-UNITDATA request shall be discarded, and an error sent to a System Manager.

Note.— The IPI designating the ISO/IEC 11577 has been included in the set of allowed IPIs in order to preserve the possiblity for use of this protocol in the future. However, at the time of publication of this specification, no ATN Security Protocol Architecture has been defined. Thus, it should be noted that this inclusion of the NLSP IPI in the allowed IPI set does not indicate that NLSP will be incorporated into the future ATN security architecture.

7.5.4.5.2. Identification of Option Parameter and Local Directory Look-up

The options part of the ISO 8473 NPDU header contained in the SN-Userdata shall then be inspected. If either of the Source Routing, Recording of Route options is present, the QOS Maintenance option is anything other than the globally unique format, padding option is present, a priority option is present with a value greater than 14, or an unknown parameter is present, then the SN-Userdata shall be sent unchanged over the virtual circuit using M-bit segmentation procedures as appropriate.

Otherwise, the local directory associated with the virtual circuit shall then be interrogated to determined if an entry exists such that:

1. the inward NSAP Address is equal to the PDU's source NSAP Address;
2. the outward NSAP Address is equal to the PDU's destination NSAP Address;
3. a security parameter is present with the same value as that contained in the PDU header, if present, and otherwise absent;
4. the same ISO 8473 version number as is present in the PDU header.

If an entry is found then the NPDU is sent in the compressed form constructed according to 7.5.4.6, using the local directory entry number as the *local reference*. If no entry is found, then a new directory entry shall be created and the SN-Userdata shall be modified as specified in 7.6.4.5.3.

7.5.4.5.3. Establishing a New Local Reference

A new directory entry shall be created containing the NPDU source NSAP Address as the inward NSAP Address, and the NPDU destination NSAP Address as the outward NSAP Address. The value of the protocol version number, and the security parameter, if present, shall also be placed in this entry. The entry number shall have the lowest possible entry number that has not previously been used for the local directory associated with this virtual circuit, and shall be in the range 0..63 or 128..16447 if the SNDCF is the initiator of the virtual circuit, or 64..127 or 16448..32767, if the SNDCF is the responder. When a directory size greater than 128 but less than 32767 has been negotiated, then the highest local reference that the initiator may allocate shall be:

127 + (n -128) / 2)

and the highest local reference that the responder may allocate shall be

16447 + (n -128) / 2)

where 'n' is the agreed maximum directory size.

If a directory full condition occurs then either the PDU shall be sent unmodified over the virtual circuit or the virtual circuit shall be reset.

Note.— A user generated Network Reset results in the total clearing of the directory which then permits the assignment of an unused local reference.

Recommendation.— *When this SNDCF is used for air-ground communication or when the local reference cancellation option is available for use, then the PDU should be sent unmodified over the virtual circuit.*

The PDU, which may be either a DT PDU or an ER PDU shall have an additional options field added to the PDU header. This option parameter shall have local significance only (i.e. is only of interest to the sending and receiving SNDCFs), and is called the Local Reference. This Local Reference option parameter shall be included as the first parameter in the Option Part of the DT or ER PDU header. This option shall be specified as follows:

Parameter Code: [0000 0101]

Parameter Length: variable

Parameter Value: the entry number of the local directory entry created above and expressed as an unsigned integer.

The checksum, Length Indicator, and Segment Length fields of the PDU header shall be modified to reflect the insertion of the new options field, and any changes to the length of the source and destination address. The Total Length, if present, shall be left unmodified.

7.5.4.5.4. Reference Cancellation Option

When the optional local reference cancellation facility is implemented and both SNDCFs using a virtual circuit have indicated that they support this facility, then the SNDCF shall monitor the number of local references on each virtual circuit, which it has both assigned and are in use. When the number of such local references on a given virtual circuit exceeds a System Manager specified threshold, then the local reference cancellation procedures specified in 7.5.4.9 shall be invoked in order to ensure that the number of unused local references in the range in which the SNDCF is permitted to assign local references, is at least equal to a System Manager specified target.

7.5.4.5.5. Transfer of the Modified ISO 8473 PDU

The modified ISO 8473 NPDU (i.e. the NPDU with the added Local Reference Option) shall be inserted in the User Data field of an ISO 8208 Data packet and shall be sent over the virtual circuit, using the ISO 8208 M-bit segmentation procedure if appropriate.

7.5.4.6. Compression of SN-Userdata

An Initial DT NPDU shall be compressed according to the procedures specified in 7.5.4.6.1. A Derived DT NPDU shall be compressed according to the procedures specified in 7.5.4.6.2. An ER NPDU shall be compressed according to the procedures specified in 7.5.4.6.3.

7.5.4.6.1. Initial DT PDU Compression

Note.— An Initial DT PDU is an ISO 8473 DT PDU that either contains no Segmentation Part in its PDU header or contains a Segmentation Part with a Segment Offset value that equals zero and the Segment Length is equal to the Total Length.

The original Initial DT PDU shall be compressed into the Compressed Initial Data PDU as shown in Figure 7.3. The fields of the Compressed Initial Data PDU will be set as follows.

7.5.4.6.1.1. Type Field

The PDU Type field value shall be set according to the values of the original Initial DT PDU ER, SP and More Segments (MS) flags as defined in Table 7-3.

Table 7-3 Initial DT PDU PDU Type codes

PDU Type Values	CLNP NPDU ER Value	CLNP NPDU SP Value	CLNP NPDU MS Value
0 0 0 0	0	0	0
0 0 0 1	0	1	0
0 0 1 0	1	0	0
0 0 1 1	1	1	0

7.5.4.6.1.2. PDU Priority Field

The PDU Priority field value shall be set to the lowest four bits of the original PDU priority parameter value field, if the priority option is present, and set to zero otherwise.

7.5.4.6.1.3. PDU Lifetime Field

The PDU Lifetime field value shall be set to the eight bits of the original NPDU lifetime field.

7.5.4.6.1.4. P bit Field

The P field value shall be set to one if the original uncompressed PDU contained the priority option. This field shall be set to zero otherwise.

7.5.4.6.1.5. Q bit Field

The Q field value shall be set to one if the original uncompressed PDU contained the QOS Maintenance option. This field shall be set to zero otherwise.

7.5.4.6.1.6. R Bit Field

The R field value shall be set to one if the original uncompressed PDU contains a non-zero checksum. This field shall be set to zero otherwise.

7.5.4.6.1.7. S/T, C/E, T/C, E/T, and E/C Fields

The values of these fields shall be set to bits 5 through 1 of the QOS parameter value option field of the original PDU, if the Quality of Service maintenance option is present.

The S/T field shall be set to the value of bit 5 of the Quality of Service Maintenance parameter value field, if present (i.e. sequencing vs. transit delay) and set to zero otherwise. The C/E field shall be set to the value of bit 4 in the Quality of Service Maintenance parameter value field. The T/C field shall be set to the value of bit 3 in the Quality of Service Maintenance parameter value field. The E/T field shall be set to the value of bit 2 in the Quality of Service Maintenance parameter value field. The E/C field shall be set to the value of bit 1 in the Quality of Service Maintenance parameter value field.

7.5.4.6.1.8. EXP, Local-REF/A and Local-REF/B Fields

If the value of the local reference determined according to the procedure specified in 7.5.4.5.3 is less than 128, then the EXP field shall be set to zero. In this case, only the Local-REF/A field shall be present in the PDU. The Local-REF/A field value shall be set to the value of the local reference encoded as an unsigned integer.

If the value of the local reference is greater than or equal to 128, the EXP field shall be set to one, and both Local-REF/A and Local-REF/B fields shall be present in the PDU. The local reference shall be encoded as a 15 bit unsigned integer, with the least significant eight bits placed in the Local-REF/B field, and the most significant seven bits placed in the Local-REF/A field.

7.5.4.6.1.9. PDU Identifier

If the Initial DT PDU allows segmentation (SP Flag is set to one), then the PDU Identifier field shall be included in the Compressed Initial Data PDU. The PDU Identifier field shall contain the Data Unit Identifier as provided in the segmentation part of the Initial DT PDU. If the Initial DT PDU does not allow segmentation (SP Flag is set to zero), then this field shall not be included in the Compressed Initial Data PDU.

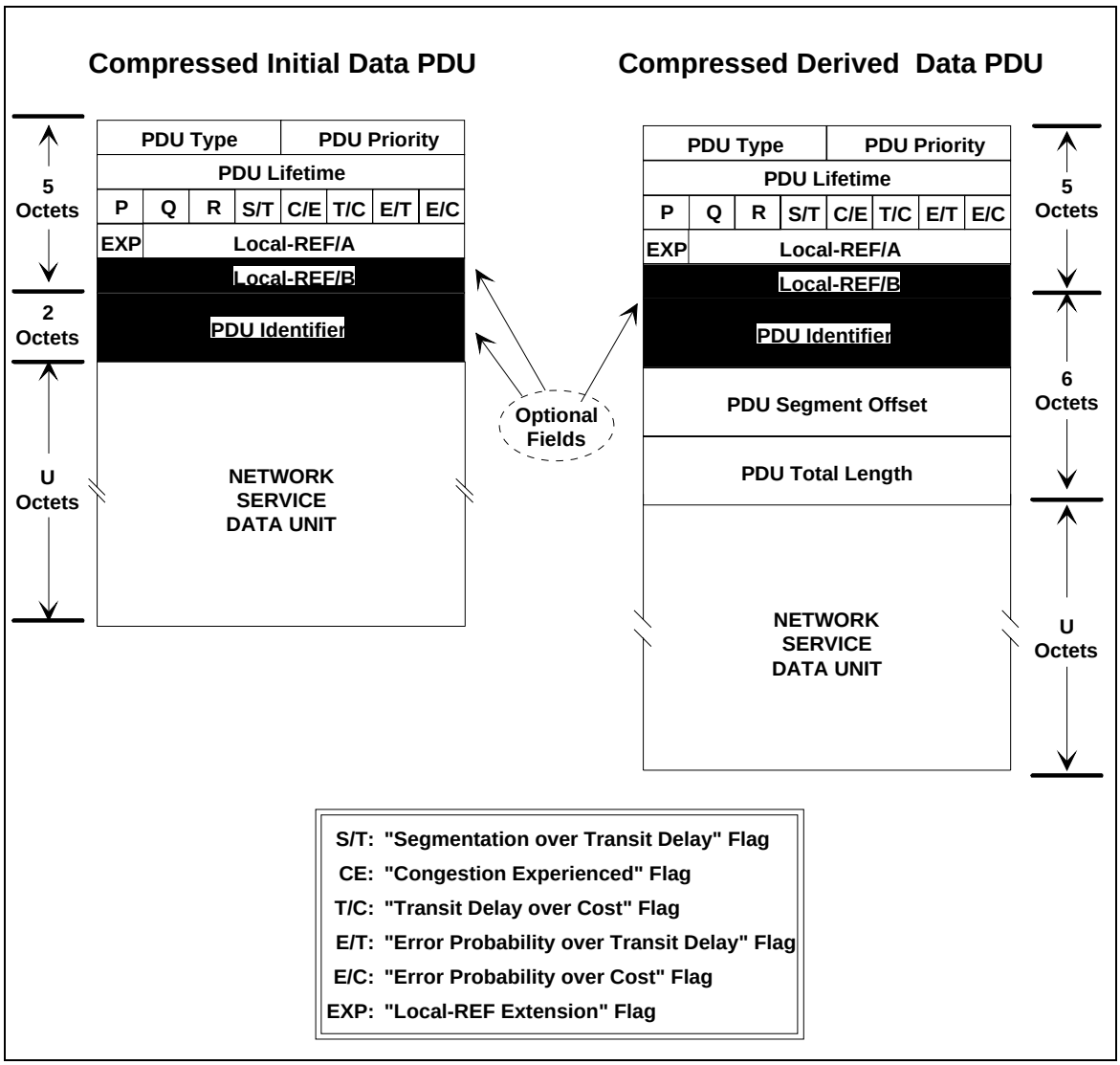


Figure 7.3: Compressed Initial and Derived PDU Formats

7.5.4.6.1.10. PDU Segment Offset

This field shall not be present in the Compressed Data PDU for an Initial DT PDU.

Note.-The segment offset of an Initial DT PDU is always zero and is a priori known by the receiving SNDCF.

7.5.4.6.1.11. PDU Total Length

This field shall not be present in the Compressed Data PDU for an Initial DT PDU.

Note.- The Total Length field value of an Initial DT PDU is the length of the entire PDU in octets. This value is identical to the value of the Segment Length field for an Initial DT PDU and both values may be recalculated by the receiving SNDCF.

7.5.4.6.1.12. Network Service Data Unit Field

This field shall contain the Data Part of the original Initial DT PDU.

7.5.4.6.2. Derived DT PDU Compression

The original Derived DT PDU shall be compressed into the Compressed Derived Data PDU as shown in Figure 7.3. The fields of the Compressed Derived Data PDU shall be set as follows.

7.5.4.6.2.1. Type Field

The PDU Type field value shall be set according to the values of the original NPDU ER, SP and MSflags as defined in Table 7-4.

Table 7-4 Derived PDU Type Codes

PDU Type Values	CLNP NPDU ER Value	CLNP NPDU SP Value	CLNP NPDU MS Value
0 1 1 0	0	1	0
0 1 1 1	0	1	1
1 0 0 1	1	1	0
1 0 1 0	1	1	1

7.5.4.6.2.2. PDU Priority Field

This field shall be set as defined in 7.5.4.6.1.2.

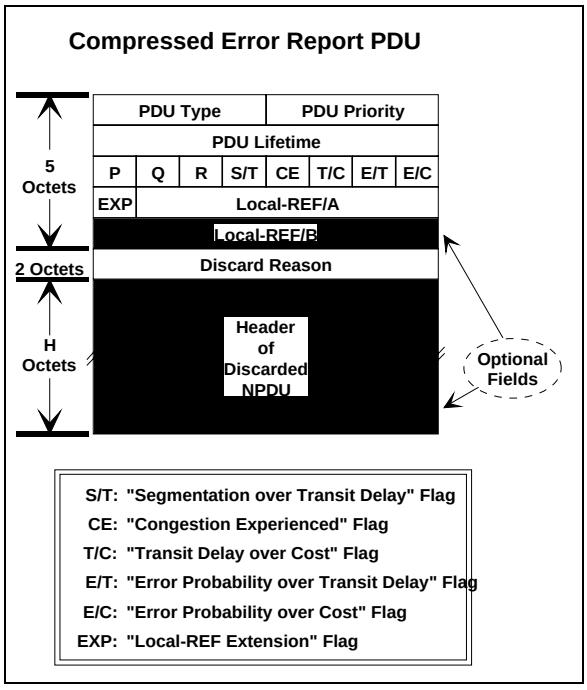


Figure 7.4: Compressed Error Report PDU

7.5.4.6.2.3. PDU Lifetime Field

This field shall be set as defined in 7.5.4.6.1.3.

7.5.4.6.2.4. P bit Field

This field shall be set as defined in 7.5.4.6.1.4.

7.5.4.6.2.5. Q bit Field

This field shall be set as defined in 7.5.4.6.1.5.

7.5.4.6.2.6. S/T, C/E, T/C, E/T, and E/C Fields

These fields shall be set as defined in 7.5.4.6.1.7.

7.5.4.6.2.7. EXP, Local-REF/A and Local-REF/B Fields

These fields shall be set as defined in 7.5.4.6.1.8.

7.5.4.6.2.8. PDU Identifier Field

The PDU Identifier field value shall be set to the Data Unit Identifier contained in the segmentation part of the original Derived DT PDU header.

7.5.4.6.2.9. PDU Segment Offset Field

The PDU Segment Offset field value shall be set to the Segment Offset value contained in the segmentation part of the original Derived DT PDU header.

7.5.4.6.2.10. PDU Total Length Field

The PDU Total Length field value shall be set to the value of the Total Length field contained in the Segmentation Part of the original Derived DT PDU.

7.5.4.6.3. Error Report PDU Compression

The original ER PDU shall be compressed into the Compressed Error Report PDU as shown in Figure 7.4. The fields of the Compressed Error Report PDU shall be set as follows

7.5.4.6.3.1. PDU Type Field

The PDU Type field value shall be set to **[1101]**.

7.5.4.6.3.2. PDU Priority Field

This field shall be set as defined in 7.5.4.6.1.2.

7.5.4.6.3.3. PDU Lifetime Field

This field shall be set as defined in 7.5.4.6.1.3.

7.5.4.6.3.4. P bit Field

This field shall be as defined in 7.5.4.6.1.4.

7.5.4.6.3.5. Q bit Field

This field shall be set as defined in 7.5.4.6.1.5.

7.5.4.6.3.6. S/T, C/E, T/C, E/T and E/C Fields

These fields shall be set as defined in 7.5.4.6.1.7.

7.5.4.6.3.7. EXP, Local-REF/A, Local-REF/B Fields

These fields shall be set as defined in 7.5.4.6.1.8.

7.5.4.6.3.8. Discard Reason Field

This field shall be set to the value of the Reason for Discard Parameter Value field contained in the original NPDU header.

7.5.4.6.3.9. Header of Discarded NPDU Field

This field shall contain the value of the Error Report Data Part if provided in the original Error Report PDU.

7.5.4.6.3.10. Transfer of Compressed ISO 8473 PDUs

The compressed ISO 8473 NPDU (i.e. Compressed Initial Data PDU, Compressed Derived Data PDU, or Compressed Error Report PDU) shall be inserted in the User Data field of an ISO 8208 Data packet and shall be sent over the virtual circuit, using the ISO 8208 M-bit segmentation procedure if appropriate.

7.5.4.7. Processing of Packets Received from the Subnetwork Service Provider

7.5.4.7.1. Initial Processing of NPDU

On receipt of an incoming packet received from a virtual circuit, the SNDCF shall inspect the first octet to determine the network layer Protocol ID or the compressed PDU type (see Table 7-5).

1. If this value is set to **[1000 0001]** indicating that the NPDU is an ISO 8473 NPDU with an uncompressed header, then the NPDU shall be processed according to 7.5.4.7.2.1.
2. If the first octet indicates either ISO 9542 (ES-IS), ISO/IEC 11577 (NLSP) or ISO/IEC 10589 (IS-IS), the SNDCF shall generate an SN-UNITDATA indication with the NPDU as its SN-Userdata parameter, and the SN-Source-Address and SN-Destination-Address parameters set to the remote and local DTE addresses for the virtual circuit over which the NPDU was received.
3. If the value of the first four bits of the first octet is in the range binary 0000 to binary 0011 then the PDU is a compressed ISO 8473 Initial DT PDU which shall be decompressed using the procedures specified in 7.5.4.7.3.
4. If the value of the first four bits of the first octet is in the range binary 0110 to binary 1010 (excluding 1000) then the PDU is a compressed ISO 8473 Derived PDU, which shall be decompressed using the procedures specified in 7.5.4.7.3.
5. If the value of the first four bits of the first octet is binary 1101 then the PDU is a compressed ISO 8473 Error PDU, which shall be decompressed using the procedures specified in 7.5.4.7.4.
6. If the value of the first four bits of the first octet is binary 1110 then the PDU is an SNDCF Error Report, which shall be processed according to the procedures of 7.5.4.7.5, and no SN-UNITDATA.indication generated.
7. If the value of the first four bits of the first octet is binary 0100 or binary 0101, then the PDU is respectively, a local reference cancellation request or response, which shall be processed according to the procedures of 7.5.4.9 and no SN-UNITDATA indication generated.

Table 7-5 Mapping between Compressed PDU Type Fields and Uncompressed PDU Types

Compressed PDU Type Field	PDU Type
[0000] - [0011]	Compressed Initial DT PDU
[0110] - [0111] [1001] - [1010]	Compressed Derived DT PDU
[1101]	Compressed Error Report PDU
[1110]	SNDCF Error Report
[0100]	Cancellation Request PDU
[0101]	Cancellation Accept PDU

In all other cases, the PDU shall be discarded and an SNDCF Error Report Generated (see 7.5.4.8).

7.5.4.7.2. Incoming ISO 8473 PDU with Uncompressed Header

If the received NPDU is an ISO 8473 NPDU then the options part shall be inspected for the options field containing the local reference.

7.5.4.7.2.1. Processing of Unmodified ISO 8473 PDUs

If the local reference option is not present, then the SNDCF shall generate a SN-UNITDATA indication with the NPDU as its SN-Userdata, and the SN-Source-Address and SN-Destination-Address parameters set to the remote and local DTE addresses for the virtual circuit over which the NPDU was received.

7.5.4.7.2.2. Processing of Modified ISO 8473 PDUs

If the local reference option is present, it shall be removed, and the checksum and PDU header

length indication and segment length shall be modified to reflect this removal.

If a local reference options field was present, then the local directory associated with the virtual circuit over which the PDU was received shall be inspected for the presence of the corresponding entry. If one is not present, and the value of the local reference is in the range within which the remote SNDCF is permitted to create local directory entries, then the entry shall be created, and:

1. The value of the inward NSAP Address set to the PDU's destination NSAP Address,
2. The value of the outward NSAP Address set to the NSAP's source NSAP Address, and
3. The values of the version number and security parameter, set to the corresponding values in the PDU header.

An SNDCF Error Report (see 7.5.4.8) shall be generated if the value of the local reference is not within the range within which the remote SNDCF is permitted to create local directory entries, or is greater than the maximum permitted and given on the call request.

Otherwise, the local directory entry shall be compared with the received PDU. If:

1. The inward NSAP Address does not match the destination NSAP Address, or
2. The outward NSAP Address does not match the source NSAP Address, or
3. The version number does not match the version number present in the directory entry, or
4. The value of the security options parameter does not match the value in the directory, or is not correspondingly absent, then

an SNDCF Error Report shall be generated and returned over the same virtual circuit as the PDU was received.

The SNDCF shall then generate a SN-UNITDATA indication with the NPDU as its SN-Userdata, and the SN-Source-Address and SN-Destination-Address parameters set to the remote and local DTE addresses for the virtual circuit over which the NPDU was received.

7.5.4.7.3. Incoming Compressed Data PDU

If the most significant four bits of the second octet of a received PDU (i.e. the PDU Type field) are in the range **[0000]** to **[0011]** binary, then the packet is a compressed ISO 8473 Initial DT NPDU. If the PDU Type field of a received compressed PDU is in the range **[0110]** to **[1010]** binary, then the PDU is a compressed ISO 8473 Derived DT NPDU. Upon receipt, the SNDCF shall examine and validate the Local-REF in the compressed PDU.

If no entry exists corresponding to the Local-REF present in the PDU , the SNDCF shall generate a SNDCF Error Report (see 7.5.4.8) and the PDU shall be discarded. This report shall be sent to the peer SNDCF via an SN-UNITDATA indication with SN-Source Address and SN-Destination-Address set to the local and remote DTE addresses for the virtual circuit, and the SN-Userdata shall contain the SNDCF Error Report. If the Local-REF is valid, the original uncompressed NPDU shall be recreated by the procedures defined in 7.5.4.7.3.1 through 7.5.4.7.3.5. The SNDCF then shall generate a SN-UNITDATA.indication with the SN-Source Address and SN-Destination Address parameters set to the remote and local DTE addresses for the virtual circuit over which the NPDU was received, and the SN-Userdata shall be set to the uncompressed DT NPDU.

7.5.4.7.3.1. Fixed Part

The Fixed Part of the NPDU header shall consist of the Network Layer Protocol Identifier, Length Indicator, Version/Protocol Identifier Extension, PDU Lifetime, SP flag, MS flag, E/R Flag, Type, Segment Length and Checksum fields as defined in ISO 8473. The value of the local reference shall be extracted from the compressed header and the corresponding entry in the local directory located. If the EXP field is set to zero, the local reference shall be the seven bit integer value of the Local-REF/A field. If the EXP field is set to one, the local reference value shall consist of the fifteen bit unsigned integer as stored with the least significant eight bits placed in the Local-REF/B field, and the most significant seven bits placed in the Local-REF/A field. The value of the Version/Protocol Identifier Extension and Source and Destination NSAP addresses shall be set the the values provided in the corresponding directory entry.

7.5.4.7.3.1.1. Network Layer Protocol Identifier

This field shall be set to binary **[1000 0001]** to identify this Network Layer Protocol as ISO 8473.

7.5.4.7.3.1.2. Length Indicator

This field shall be set to the length of the uncompressed NPDU header in octets.

7.5.4.7.3.1.3. Version/Protocol Identifier Extension

The Version/Protocol Identifier Extension field shall be extracted from the corresponding entry in the local directory.

7.5.4.7.3.1.4. PDU Lifetime

The eight bits of the PDU Lifetime Field shall be set to the eight bits of the PDU lifetime field of the Compressed Data PDU.

7.5.4.7.3.1.5. Segmentation Permitted, More Segments, Error Report Flags

The values of these flags shall be based upon the value of the Protocol ID field and Type field of the Compressed Data PDU. These flag values shall be determined according to Table 7-3 for an Initial Data PDU and Table 7-4 for a Derived Data PDU.

7.5.4.7.3.1.6. Type Code

This field shall be set to binary **[11100]** to indicate a DT PDU.

7.5.4.7.3.1.7. Segment Length

This field shall indicate the entire length in octets of the PDU, including both header and data. The value of this field shall be computed by the SNDCF. For an Initial DT NPDU, the value of this field shall be identical to the value of the Total Length field located in the Segmentation Part of the header.

7.5.4.7.3.1.8. PDU Checksum

The value of this field shall be set to zero if the R Bit in the compressed header is zero. Otherwise, a checksum field will be recomputed.

Note.— For the DT PDU, this includes the segmentation and options part (if present). For the Error Report PDU, this includes the reason for discard field as well.

7.5.4.7.3.2. Address Part

The Address Part shall consist of the Destination Address Length Indicator, Destination Address, Source Address Length Indicator and Source Address as defined in ISO 8473.

7.5.4.7.3.2.1. Destination and Source Address Length Indicators and Addresses

The Source and Destination NSAP addresses shall be extracted from the corresponding entry in the local directory for the local reference number calculated. The source NSAP Address shall be set to the value of the outward NSAP Address, and the destination NSAP Address shall be set to the value of the inward NSAP Address. The length fields shall contain the length of each address in octets.

7.5.4.7.3.3. Segmentation Part

If the ISO 8473 SP field is set to one, then the Segmentation Part shall be generated. The Segmentation Part shall consist of the Data Unit Identifier, Segment Offset, and Total Length field as defined in ISO 8473.

7.5.4.7.3.3.1. Data Unit Identifier

This field shall contain the value of the PDU Identifier field as provided in the compressed DT PDU.

7.5.4.7.3.3.2. Segment Offset

For an Initial DT PDU, this field shall be set to zero. For a Derived DT PDU, this field shall be set to the PDU Segment Offset field as provided in the compressed DT PDU.

7.5.4.7.3.3.3. PDU Total Length

For a Derived DT PDU, this field shall contain the value of the PDU Total Length field as provided in the Compressed DT PDU. For an Initial PDU, the entire length of the PDU in octets shall be calculated by the SNDCF and stored in this field.

7.5.4.7.3.4. Options Part

If the Q bit field is set to one, the Globally Unique QoS option shall be recreated according to 7.5.4.7.3.4.2. If the Security option is present in the local reference directory entry, the Security option shall be recreated according to 7.5.4.7.3.4.3. If the P bit field is set to one, the Priority option shall be recreated according to 7.5.4.7.3.4.1.

7.5.4.7.3.4.1. Priority

For the Priority option, the Parameter Code shall be set to binary **[1100 1101]** and the Parameter Length shall be set to one octet. The four most significant bits of the Parameter Value shall be set to zero, and the four least significant bits shall be set to the PDU Priority field as provided in the compressed DT PDU.

7.5.4.7.3.4.2. Quality of Service Maintenance

For the Quality of Service Maintenance option, the Parameter Code shall be set to binary **[1100 0011]**, the Parameter Length shall be set to one octet. The high order two bits of the Parameter Value shall be set to binary **[11]** to indicate Globally Unique, bit 6 shall be set to zero, and bits 5 through one shall be set to the S/T, C/E, T/C, E/T and E/C fields respectively as provided in the compressed Data PDU.

7.5.4.7.3.4.3. Security

This field shall be set to the security parameter contained in the corresponding local reference directory entry.

7.5.4.7.3.5. Data Part

The Data Part shall contain the NSDU as provided in the Compressed Data PDU.

7.5.4.7.4. Incoming Compressed Error Report PDU

The original uncompressed header shall be recreated as follows.

*Note.— If the four most significant bits of the first octet (the PDU Type Field) of a received packet are **[1101]** then the packet is a compressed ISO 8473 ER NPDU.*

7.5.4.7.4.1. Fixed Part

The Fixed Part of the ER PDU shall be composed in the same manner as defined in 7.5.4.7.3.1 except for the Type Code which shall be set to binary **[1101]** to indicate an ER PDU, and except for the SP and MS flags which shall be set to zeros.

7.5.4.7.4.2. Address Part

The Address Part of the ER PDU shall be composed in the same manner as defined in 7.6.4.7.3.2.

7.5.4.7.4.3. Options Part

The Options Part of the ER PDU shall be composed in the same manner as defined in 7.5.4.7.3.4 for an Initial DT PDU.

7.5.4.7.4.4. Reason for Discard

To compose this field, the Parameter Code shall be set to binary **[1100 0001]**, the Parameter Length shall be set to two octets, and the Parameter Value shall contain the Discard Reason field as provided in the Compressed Error Report PDU.

7.5.4.7.4.5. Error Report Data Part

If the Compressed Error Report PDU contains the Header of Discarded NPDU field, then the Error Report Data Part shall be set to the value of the Header of Discarded NPDU field.

7.5.4.7.5. Incoming SNDCF Error Report

On receipt of an SNDCF Error Report, the virtual circuit shall be reset (see 7.5.4.11), and systems management informed of the problem, unless the reason is "compressed PDU with unrecognized local reference".

In this case, the directory entry corresponding to the local reference returned in the SNDCF Error Report shall be reset to the unused state, and the error should be notified to Systems Management.

*Note.— If the four most significant bits of the first octet (the PDU Type field) of an incoming packet are set to **[1110]**, then a SNDCF Error Report has been received (see 7.*5.4.8*).*

7.5.4.8. SNDCF Error Report

The SNDCF Error Report is a packet format unique to the Mobile SNDCF, and shall be used to report errors in the use of local references as specified below. The SNDCF Error Report PDU shall be constructed as follows:

1. The most significant four bits (PDU Type) of the first octet are set to binary 1110, while the least significant four bits are set to 0000.
2. The second octet is a discard reason encoded as an unsigned integer, with the following reason codes defined:
   a) reason = **[0000 0000]** - compressed NPDU with unrecognized local reference
   b) reason = **[0000 0001]** - creation of directory entry outside of sender's permitted range
   c) reason = **[0000 0010]** - directory entry exists
   d) reason = [**0000 0011**] - local reference greater than maximum value accepted.
   e) reason = [**0000 0100**] - Data Unit Identifier missing when SP=1.
   f) reason = **[0000 0101]** - reserved~~PDU with unrecognized Protocol ID~~.
   g) reason = **[0000 0111]** - Compressed ISO 8473 PDU with unrecognized Type.
   h) reason = [**0000 1000**] - local reference cancellation error
3. The local reference contained in the PDU for which the error is being reported is placed in the remaining octet(s) of the SNDCF Error Report PDU Header, unless the reason is *local reference cancellation error*, when the SNDCF Error Report shall consist of three octets only, and the third octet shall contain the Cancellation Reference of the invalid Cancellation Request PDU.

The data portion of the SNDCF Error Report shall be used to return a copy of the PDU in error, similarly to the ISO 8473 Error Report PDU. The Error Report PDU shall be sent as an ISO 8208 DATA packet(s) and, if needed, segmented using the M-bit procedures.

7.5.4.9. Local Reference Cancellation Option

Note.— When the implementation of this option has been agreed by both SNDCFs using a virtual circuit during the call setup procedures, then the following procedures may be used to selectively cancel one or more local references i.e. make them available for re-use. An SNDCF may only

request the cancellation of local references which are within the range in which it is permitted to assign local references.

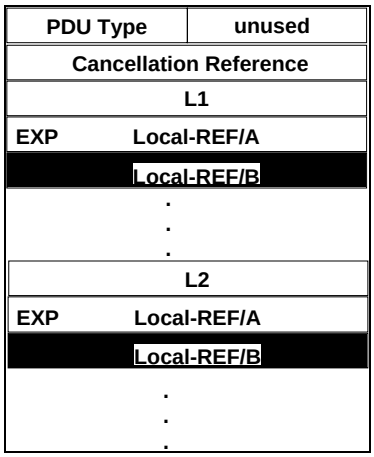


Figure 7.5: Cancellation Request PDU

When an SNDCF invokes the procedures for local reference cancellation it shall format a *cancellation request PDU*, as specified below, and shall send the PDU to the other SNDCF over the virtual circuit to which it applies. A cancellation request PDU shall be retransmitted periodically until it is acknowledged by a *cancellation accept PDU*, or an SNDCF Error Report PDU is received indicating an error in the request. When a cancellation accept PDU is received, the corresponding local references are now available for re-use and the corresponding directory entries may be cleared.

When an SNDCF receives a cancellation request PDU, it shall first check to ensure that the local references identified in the PDU are within the range in which the sending SNDCF is permitted to assign local references. If any one of them is not, then an SNDCF error report shall be returned, and the request ignored. Otherwise, the directory entries corresponding to the indicated local references shall be cleared, and a cancellation accept PDU shall be formatted and returned, in order to accept cancellation of these local references.

7.5.4.9.1. The Cancellation Request PDU

The PDU format is illustrated in Figure 7.5. The first octet shall be set to [**0100 0000**] . The remainder of the PDU shall consist of:

1. A cancellation reference expressed as a one octet unsigned integer, and which uniquely identifies this cancellation request within the context of the virtual circuit.

Note 1.— In most cases uniqueness will be assured if the reference is implemented as a sequence number starting at zero and incremented by one (MOD 256), each time a cancellation request is sent.

2. A length octet (L1) given as an unsigned integer (0 to 255), the length in octets of the set of individual local references to cancel.
3. One or more local references expressed as one or two octets each, as appropriate, and encoded in successive octets, with the total number of octets containing such local references given by L1.
4. A length octet (L2) given as an unsigned integer (0 to 255), the length in octets of the set of inclusive local reference ranges to cancel.
5. One or more pairs of local reference ranges expressed as one or two octets each, as appropriate, and encoded in successive octets, with the total number of octets containing such local references given by L2.

In each of the above cases, if the value of a local reference is less than 128, then bit eight of the first octet in which it is encoded is set to zero, and the remaining seven bits set to the value of the local reference encoded as an unsigned integer. The extended local reference octet is not present. Otherwise, bit eight is set to one, and the remaining seven bits and the next octet are set to the value of the local reference encoded as a 15 bit unsigned integer, with the least significant eight bits placed in the extended local reference octet, and the most significant seven bits placed in the first octet.

Note 2.— This format allows for the local references to cancel to be expressed as either a set of individual references to be cancelled, or a set of inclusive ranges of individual references to be cancelled, or both.

7.5.4.9.2. The Cancellation Accept PDU

The PDU format is illustrated in Figure 7.6. The first octet shall be set to binary 0101 0000, and the second octet shall contain the Cancellation Reference of the cancellation request which is being accepted.

7.5.4.10. Call Clearing Provisions

The Mobile SNDCF shall clear a virtual circuit when:

1. System management requests call

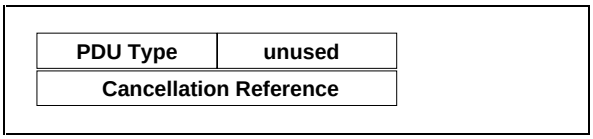


Figure 7.6: Cancellation Accept PDU

Table 7-6 Diagnostics values for ATN call clearing

	Hexadecimal value	Decimal value	
1	1111 1001	249	Connection Rejection - unrecognized protocol identifier in user data
2	1000 0000	128	Version number not supported
3	1000 0001	129	Length field invalid
4	1000 0010	130	Call Collision Resolution
5	1000 0011	131	Proposed Directory Size too large
6	1000 0100	132	Local Reference Cancellation Not Supported
7	1000 0101	133	Received DTE refused, received NET refused or invalid NET selector
8	1000 0110	134	Invalid SNCR field
9	1000 0111	135	ACA compression not supported
10	1000 1111	143	V42bis compression not supported
11	1111 0000	240	System lack of resources
12	0000 0000	0	Cleared by System Management
13	1001 0000	144	Idle Timer expiration
14	1001 0001	145	Need to re-use the circuit
15	1001 0010	146	By local means (to be used for system local error)
16	1001 0011	147	Invalid NSEL in received NET

clearing, or

2. The expiration of a timeout period following the transmission or receipt of SN-UNITDATA, or

3. The resources are required by another virtual circuit with a higher priority.

Options 2 or 3 above shall only apply to those virtual circuits that have been dynamically established (see 7.5.4.5). When it has been determined that a virtual circuit shall be cleared, the SNDCF shall perform all functions associated with call clearing. All packets received other than a Clear Confirm or a Clear Indication shall be ignored. The same actions shall apply to the receipt of a Clear Indication.

When a virtual circuit has been terminated, then the local directory associated with the virtual circuit shall be discarded.

The value of the cause octet in the ISO-8208 cause/diagnostic field which shall be used is 1000 0000 The reason for clearing the code is placed in the diagnostic field . The diagnostic values listed in Table 7-6 shall be used when an SNDCF rejects a Call Request or clears a virtual circuit.

Note.— If a virtual connection is cleared due to a network problem, the SNDCF may attempt to re-establish the connection before the associated forwarding information is removed from network layer routing tables. The selective re-establishment of X.25 connections may be based on the originating clearing cause and diagnostic codes.

7.5.4.11. Call Reset Provisions

If at any time, a reset indication is received indicating a DCE originated reset, then this shall be confirmed and all other procedures associated with the call reset performed. Otherwise, there shall be no impact on this SNDCF.

If the reset indication indicates a DTE originated reset then, additionally, the directory associated with the virtual circuit shall be cleared to its initial state.

7.6. Convergence Provisions for ISO 8802-2 Broadcast Subnetworks

The subnetwork service specified in 7.1 shall be provided using ISO 8802-2 Broadcast Subnetworks as specified in Clause 8.4.2 of ISO 8473.

7.7. Convergence Provisions for Common ICAO Data Interchange Network (CIDIN)

7.7.1. General Considerations

Note.— CIDIN provides a connectionless transmission service so that the functionality provided by CIDIN at level 4 is already very close to what is required by the ATN network protocol.

7.7.2. Mapping of the ATN Service Primitives to CIDIN

The relationship between the ATN subnetwork primitives, their parameters, and the CIDIN protocol parameters shall be as follows.

7.7.2.1. SN-UNITDATA Request and Indication Primitives

These primitives shall correspond to the request to send a CIDIN message at a CIDIN entry centre and the reception of a CIDIN message at a CIDIN exit centre respectively. CIDIN messages shall be sent with the "no acknowledgement" option.

Note.— CIDIN messages requested to be transported to exit addresses which are not reachable are discarded in the entry centre.

7.7.2.2. SN Source Address

This address shall correspond to a CIDIN entry address in the entry address item.

7.7.2.3. SN Destination Address

This address shall correspond to a CIDIN exit address in an exit address item.

7.7.2.4. SN Quality of Service

A priori values for transit delay, protection against unauthorized access, cost determinants and residual error probability shall be entered as management data in the ATN system~~router~~.

7.7.2.5. SN Priority

The mapping between SN Priority and the CIDIN subnetwork priority shall be entered as management data in the ATN system~~router~~.

7.7.2.6. SNS-Userdata

SNS-Userdata shall be conveyed as the contents of the CIDIN message which is transported transparently by CIDIN.

Note.— The coding of the CIDIN message is code and byte independent.

7.8. ATN NSAP Compression Algorithm (ACA)

7.8.1. General Overview

The optional ACA compression processing (7.8.5) shall be applied to data octets being output to the subnetwork, while ACA decompression processing (7.8.6) shall be applied to data octets input from the subnetwork.

7.8.2. Address Length Determination

The address length for the address or address prefix to be compressed shall be extracted from the octet preceding the AFI octet in the uncompressed data stream. If the extracted length lies in the range 7 through 20, the extracted length shall be used as the address "octet length" and the address length type shall be indicated as "normal". If the extracted length lies in the range 56 through 160 and is an integral multiple of 8, the extracted length shall be divided by 8 to compute the length in octets of the address prefix and the address length type shall be indicated as "IDRP". If the extracted length does not lie in either of these ranges, the input data does not form a compressible ATN address and the ACA shall not further process the current data as a compressible ATN address.

The octet length for ACA compressed address prefixes shall be encoded in the first header octet LEN/SEL subfield and the FP subfield shall be set to one. If the octet length for the ACA compressed address is 20 (indicating a full address instead of a prefix) the FP subfield shall be set to zero. The explicit address length octet shall be removed as part of the ACA compression processing.

Note 1.— No length octet is required for compressed ACA addresses. All information concerning address length and the presence or length of variable-length fields is contained in the header octets.

Note 2.— The shortest ATN address prefix that can be compressed is 7 octets and the length of a full ATN address is 20 octets.

Note 3.— Address lengths for normal addresses and prefixes are expressed in octet units. The address lengths for IDRP addresses and prefixes

are expressed in bit units (even though the address lengths are always in full octets).

Note 4.—The IDRP subfield in the first header octet indicates whether the expanded address used octet or bit length units. Internal (compressed) addresses assume octet lengths for encoding.

7.8.3. Compressed Address Structure

An ACA compressed address or address prefix shall consist of the following components in the order shown below:

Name	Length (octets)	Reference
Address Marker	2	7.9.4
Header Octet 1	1	7.9.3.1.1
Header Octet 2	1	7.9.3.1.2
Compressed ADM	2 or 3	7.9.3.2
Variable Fields	0 to 14	7.9.3.3

The coding and use of each component shall be as defined below.

Note.— Multi-octet uncompressed ATN address fields (ADM, ARS, LOC, and SYS) are processed from left to right, i.e. from most-significant to least-significant octet.

7.8.3.1. Address Header Octets

Two header octets shall begin each compressed address or address prefix. All bits of these header octets shall be set to zero unless otherwise specified in the following subparagraphs. Bits in each header octet shall be assigned from the high-order (most-significant or left-most).

Note.— The value of the first header octet is never zero for any compressed address. This prevents confusing a compressed address with an embedded address marker (7.8.4.2).

7.8.3.1.1. First Header Octet

The first header octet of a compressed address shall be subdivided into four subfields as follows:

Name	Nb of bits	Comments
IDRP	1	Units of address length
FP	1	Full address of prefix
LEN/SEL	3	Address length or SEL code
CVER	3	Compressed VER value

The coding and use of each subfield shall be as defined below

7.8.3.1.1.1. IDRP Subfield

If the address length determination process (7.8.1, 7.8.2) indicates that the address to be compressed expresses length in octet units, the IDRP subfield shall be set to zero. If the address expresses length in bit units (i.e. IDRP address), the IDRP subfield shall be set to one.

7.8.3.1.1.2. FP Subfield

The FP subfield shall be set to one if the address to be compressed is an address prefix. The FP subfield shall be set to zero if the address to be compressed is a full address (i.e. its octet length is 20).

7.8.3.1.1.3. LEN/SEL Subfield

If the address to be compressed is an address prefix (the FP subfield is set to one), the LEN/SEL subfield shall be set to the the prefix length encoded using the encodings in the following table:

Length	Encoding	Comments
--	0	reserved
7	1	end with ADM
8	2	end with RDF
11	3	end with ARS
13	4	end with LOC
19	5	end with SYS
--	6, 7	unassigned

If the length is not found in this encoding table then the input data does not form an ATN address prefix that can be compressed and the address prefix shall not be further processed.

If the address to be compressed is a full address (the FP subfield is set to zero), the LEN/SEL subfield shall be set to the encoded value of the address SEL field (4.5.9.3) using encodings in the following table:

SEL	Encoding	Comments
--	0	reserved
00 hex	1	NET
fe hex	2	NET of an airborne router not supporting IDRP
--	3, 4, 5, 6	unassigned
--	7	other SEL codes

If the SEL field value in the address to be compressed is not one of the table entries above, the LEN/SEL encoding value shall be set to 7.

Note .— A LEN/SEL subfield value of zero is not allowed in either encoding to insure that the first header octet can never have the value [00] hexadecimal. Hence, no compressed address can be confused with an embedded address marker (7.8.4.2).

7.8.3.1.1.4. CVER Subfield

If the value of the VER field in the address is in the range [01]-[07], [41]-[47], [81]-[87], or [c1]-[c7], then the CVER subfield shall be set to the low-order 3 bits of the VER value. If the value of the VER field in the address is not in one of the above ranges, then the CVER subfield shall be set to zero.

Note.— The encoding of the version numbers in ATN addresses is defined in 4.5.3.4.

7.8.3.1.2. Second Header Octet

The second header octet of a compressed address shall be subdivided into 8 subfields as follows:

Name	Nb of bits	Comments
ADMF	1	Flag compressed ADM value
T/I	1	ATSC/AINSC
F/M	1	Fixed/Mobile
ARSD	1	Flag defaulted ARS value
LOCD	1	Flag defaulted LOC value
SYS6	1	Flag octet 6 of SYS = 0
SYS5	1	Flag octet 5 of SYS = 0
SYS4	1	Flag octet 4 of SYS = 0

The encodings and use of each subfield shall be as defined below.

7.8.3.1.2.1. ADMF Subfield

The ADMF subfield shall be set to one if the ADM value in the address to be compressed may be encoded into two octets using the identifier metacharacter syntax (4.4.7). The ADMF subfield shall be set to zero if the ADM value in the address to be compressed cannot be expressed using the identifier metacharacter syntax.

Note.— The ADM value can be compressed if each of its three octets contain a character from one of the following character classes:

a) An upper-case letter "A-Z"

b) A decimal digit "0-9"

c) The "@" character.

7.8.3.1.2.2. T/I Subfield

The T/I subfield shall be set to zero if the VER value in the address to be compressed lies in the ranges [01]-[3f] or [41]-[7f], indicating that the address is in the AINSC domain. The T/I subfield shall be set to one if the VER value in the address to be compressed lies in the ranges [81]-[bf] or [c1]-[ff], indicating that the address is in the ATSC domain. If the VER value in the address to be compressed is either [00], [40], [80], or [c0], then the T/I subfield shall be set to zero.

Note. .— The encoding of the VER field in an ATN address is defined in 4.5.3.3.

7.8.3.1.2.3. F/M Subfield

The F/M subfield shall be set to zero if the VER value in the address to be compressed lies in the ranges [01]-[3f] or [81]-[bf], indicating that the address is a fixed system. The F/M subfield shall be set to one if the VER value in the address to be compressed lies in the ranges [41]-[7f] or [c1]-[ff], indicating that the address is a mobile system.

Note.— The values [00], [40], [80] and [c0] are not used in the VER field of an ATN address (see 4.5.3.3)

7.8.3.1.2.4. ARSD Subfield

The ARSD subfield shall be set to zero if the ARS value in the address to be compressed is not the default value ([000001] hexadecimal) or if the address prefix to be compressed does not include an ARS field. The ARSD subfield shall be set to one if the ARS value in the address to be compressed has the default value (4.5.6.5).

7.8.3.1.2.5. LOCD Subfield

The LOCD subfield shall be set to zero if the LOC value in the address to be compressed is not the default value ([0001] hexadecimal) or if the address prefix to be compressed does not include a LOC field. The LOCD subfield shall be set to one if the LOC value in the address to be compressed has the default value (4.5.7.5).

7.8.3.1.2.6. SYS6 Subfield

The SYS6 subfield shall be set to zero if the value of the high-order (6th) octet of the SYS field in the address to be compressed is zero or if the address prefix to be compressed does not include a SYS field. The SYS6 subfield shall be set to one if the value of the high-order (6th) octet of the SYS field in the address to be compressed is nonzero.

7.8.3.1.2.7. SYS5 Subfield

The SYS5 subfield shall be set to zero if the value of the second to high-order (5th) octet of the SYS field in the address to be compressed is zero or if the address prefix to be compressed does not include a SYS field. The SYS5 subfield shall be set to one if the value of the second to high-order (5th) octet of the SYS field in the address to be compressed is nonzero.

7.8.3.1.2.8. SYS4 Subfield

The SYS4 subfield shall be set to zero if the value of the third to high-order (4th) octet of the SYS field in the address to be compressed is zero or if the address prefix to be compressed does not include a SYS field. The SYS4 subfield shall be set to one if the value of the third to high-order (4th) octet of the SYS field in the address to be compressed is nonzero.

7.8.3.2. Compressed ADM Field

If the ADM field value of the address to be compressed follows the syntax of an identifier (4.4.7) then the compressed ADM field shall consist of two octets and shall contain the encoded value of the identifier obtained by applying the definitions in 4.4.7 to the ADM field value. If the ADM field value of the address to be compressed does not follow the identifier syntax then the compressed ADM field shall consist of three octets and shall contain the 3-octet ADM value unchanged.

Note.— The value of the ADMF subfield in the second header octet indicates whether the compressed ADM field has the 2-octet (compressed) or 3-octet (uncompressed) format.

7.8.3.3. Variable Fields

The variable fields shall have a minimum length of 0 octets and a maximum length of 13 octets. Variable field data octets shall be concatenated when required in the order that their fields occur in the ATN address (Figure 7.2) as follows:

a) VER value (if > 7), 1 octet

b) ARS value (if not default), 3 octets

c) LOC value (if not default), 2 octets

d) SYS octet 6 value (if nonzero), 1 octet

e) SYS octet 5 value (if nonzero), 1 octet

f) SYS octet 4 value (if nonzero), 1 octet

g) SYS octets 3-1, 3 octets

h) SEL value (if not defined in 4.5.9.3), 1 octet

The ACA compression of address prefixes shall omit those variable fields b) through h) which are not present in the uncompressed address prefix.

7.8.4. Compressed Address Marker

The ACA shall prefix each compressed address or address prefix with an address marker. The address marker shall consist of two octets with the value [55aa] hexadecimal. The ACA shall process the case of the address marker value occuring in the input octet stream as defined in 7.8.4.2 below.

7.8.4.1. Normal Address Case

In the case of a normal compressed address or address prefix, the header octets of the compressed address format (7.8.3) shall follow the address marker.

Note.— The first header octet of a compressed address can never have the value [00]. This distinguishes the normal address case from the embedded address case.

7.8.4.2. Embedded Address Marker Case

If two octets with the value of an address marker occur in data, a padding octet with value [00] hexadecimal shall be inserted into the data stream following the embedded address marker octets.

Note 1.—The likelihood of embedded address markers in the input data stream is very low. When they occur, however, the ACA algorithm must add the extra padding octet. Hence, it is possible (although highly unlikely) for the ACA to expand data.

Note 2.— The design of the ACA requires that the first header octet of a compressed address can never have the value [00] hexadecimal. Hence, the first header octet of a compressed address cannot be confused with the padding octet of an embedded address marker.

7.8.5. Compression Algorithm

The ACA shall perform compression by replacing ATN addresses or address prefixes identified in the input octet stream with compressed, encoded equivalents as defined below. The format of a compressed address shall be as defined in 7.8.3. Each compressed address shall be prefixed with a compressed address marker (7.8.4). Any embedded address markers found in the input octet stream shall be padded with a null-value octet (7.8.4.2). The overall logic flow of the ACA compression processing shall be as defined in 7.9.5.2.

7.8.5.1. Address Encoding Process

The process of encoding an ATN address or address prefix into the ACA compressed format (7.8.3) shall be performed using the sequence of steps defined in this paragraph. The steps shall be performed in the order they are listed. If any step of the encoding process fails, the ACA compression processing shall not consider the current input octets as an address and shall continue with the compression logic.

7.8.5.1.1. Encoding Address Length

Determination of the length in octets of an address to be compressed shall be performed as defined in 7.8.1, 10.9.2. If the address length is of type

"normal", the IDRP subfield in the first header octet shall be set to zero. Otherwise, the IDRP subfield shall be set to one.

If the octet length of the address is 20 (indicating a full ATN address), the FP subfield in the first header octet shall be set to zero. If the octet length of the address is less than 20 (indicating an address prefix), the FP subfield shall be set to one and the address length shall be encoded in the LEN/SEL subfield of the first header octet according to the table in 7.8.3.1.1.3. If the address length is not found in the length table, the encoding process shall halt and the current input octet string shall not be treated as an ATN address.

7.8.5.1.2. Encoding the AFI and IDI Fields

No encoding shall be performed on the constant values of the address AFI and IDI fields. These fields shall be omitted from the compressed address encoding.

7.8.5.1.3. Encoding the VER Field

If the VER value in the address to be compressed lies within the range [01]-[3f], the T/I subfield in the second header octet shall be set to zero and the F/M subfield in the second header octet shall be set to zero. If the VER value lies within the range [01]-[07], then the low-order 3 bits of the VER value shall be stored in the CVER subfield of the first header octet. If the VER value lies in the range [08]-[3f], then the CVER subfield shall be set to zero and the VER value octet shall be concatenated to the variable field of the encoded address.

If the VER value in the address to be compressed lies within the range [41]-[7f], the T/I subfield in the second header octet shall be set to zero and the F/M subfield in the second header octet shall be set to one. If the VER value lies within the range [41]-[47], then the low-order 3 bits of the VER value shall be stored in the CVER subfield of the first header octet. If the VER value lies in the range [48]-[7f], then the CVER subfield shall be set to zero and the VER value octet shall be concatenated to the variable field of the encoded adress.

If the VER value in the address to be compressed lies within the range [81]-[bf], the T/I subfield in the second header octet shall be set to one and the F/M subfield in the second header octet shall be set to zero. If the VER value lies within the range [81]-[87], then the low-order 3 bits of the VER value shall be stored in the CVER subfield of the first header octet. If the VER value lies in the range [88]-[bf], then the CVER subfield shall be set to zero and the VER value octet shall be concatenated to the variable field of the encoded adress.

If the VER value in the address to be compressed lies within the range [c1]-[ff], the T/I subfield in the second header octet shall be set to one and the F/M subfield in the second header octet shall be set to one. If the VER value lies within the range [c1]-[c7], then the low-order 3 bits of the VER value shall be stored in the CVER subfield of the first header octet. If the VER value lies in the range [c8]-[ff], then the CVER subfield shall be set to zero and the VER value octet shall be concatenated to the variable field of the encoded adress.

If the VER value is either [00], [40], [80], or [c0], the encoding process shall halt and the current input octet string shall not be treated as an ATN address.

7.8.5.1.4. Encoding the ADM Field

If the three octets of the ADM field in the address to be compressed do not follow the rules for Identifier Syntax (4.4.7), the ADMF subfield in the second header octet shall be set to zero and the three octets of the ADM field value shall be concatenated to the compressed ADM of the encoded address. If the ADM field value does follow the Identifier Syntax rules, the ADMF subfield shall be set to one and the two-octet compressed ADM value (7.8.3.2) shall be concatenated to the compressed ADM of the encoded address.

7.8.5.1.5. Encoding the RDF Field

If the address length indicates an address prefix whose length is less than or equal to 7, no RDF field value shall be encoded and the encoding process shall halt.

If the RDF value in the address to be compressed is not [00], the encoding process shall halt and the current input octet string shall not be treated as an ATN address.

7.8.5.1.6. Encoding the ARS Field

If the address length indicates an address prefix whose length is less than or equal to 8, no ARS field value shall be encoded and the encoding process shall halt.

If the ARS value of the address to be compressed has the default value ([000001] hexadecimal), the ARSD subfield in the second header octet shall be set to one. If the ARS value of the address to be compressed is not default, the ARSD subfield shall be set to zero and the three octets of the ARS value shall be concatenated to the variable field data of the encoded address.

7.8.5.1.7. Encoding the LOC Field

If the address length indicates an address prefix whose length is less than or equal to 11, no LOC field value shall be encoded and the encoding process shall halt.

If the LOC value of the address to be compressed has the default value ([0001] hexadecimal), the LOCD subfield in the second header octet shall be set to one. If the LOC value of the address to be compressed is not default, the LOCD subfield shall be set to zero and the two octets of the LOC value shall be concatenated to the variable field data of the encoded address.

7.8.5.1.8. Encoding the SYS Field

If the address length indicates an address prefix whose length is less than or equal to 13, no SYS field value shall be encoded and the encoding process shall halt.

If the high-order (6th) octet of the SYS field of the address to be compressed has a nonzero value, the SYS6 subfield in the second header octet shall be set to zero and the value of the SYS field octet shall be concatenated to the variable field data of the encoded address. Otherwise, the SYS6 subfield shall be set to one.

If the second to high-order (5th) octet of the SYS field of the address to be compressed has a nonzero value, the SYS5 subfield in the second header octet shall be set to zero and the value of the SYS field octet shall be concatenated to the variable field data of the encoded address. Otherwise, the SYS5 subfield shall be set to one.

If the third to high-order (4th) octet of the SYS field of the address to be compressed has a nonzero value, the SYS4 subfield in the second header octet shall be set to zero and the value of the SYS field octet shall be concatenated to the variable field data of the encoded address. Otherwise, the SYS4 subfield shall be set to one.

The three remaining octets of the SYS field shall be concatenated to the variable field data of the encoded address.

7.8.5.1.9. Encoding the SEL Field

If the address length indicates an address prefix whose length is less than or equal to 19, no SEL field value shall be encoded and the encoding process shall halt.

Since the address length indicates a full ATN address, the FP subfield in the first header octet shall be set to zero. The SEL value shall be encoded into the LEN/SEL subfield in the first header octet according to the table in 7.8.3.1.1.3. If the SEL value is not one of the table entries, the LEN/SEL subfield shall be set to 7 and the SEL value octet shall be concatenated to the variable field data of the encoded address.

7.8.5.2. Compression Logic Flow

The ACA compression logic shall process octets sequentially from the uncompressed data input stream. For each input octet, a test shall be performed to determine if the current octet and the subsequent octets form an ATN address or address prefix. If they do form an ATN address, the ACA shall attempt to encode the address into the compressed address format (7.8.3) as defined in the steps of 7.8.5.1.

If the encoding process is successful, a compressed address marker (7.8.4) shall be output to the compressed octet stream followed by the compressed address octets. The compression processing shall then continue with the next uncompressed data octet not a part of the address just processed.

If the encoding process fails, or if the current octet does not begin an ATN address, the ACA processing shall check at the current uncompressed octet position in the input data stream for an embedded address marker (7.8.4.2). If an embedded address marker is found, the ACA shall copy the address marker octets to the compressed output octet stream. A padding zero-valued octet shall be output as well as the address marker. The compression processing shall then continue with the next uncompressed data octet not a part of the embedded address marker.

If neither an ATN address or embedded address mark is found, the ACA shall copy the current uncompressed input octet to the compressed output octet stream and shall continue processing with the next sequential input octet.

Note.— Since the ACA compression logic may not recognize the appearance of an ATN address or prefix in the data stream until after the uncompressed length octet has been processed (the length octet precedes the fixed-value ATN AFI and IDI fields that distinguish an ATN address), the ACA compression process will need to be able to recall the value of the previous input octet during compression processing. Hence, a one-octet "backup" may be necessary in the implementation of the ACA compression logic.

7.8.6. Decompression Algorithm

The ACA shall perform decompression by replacing compressed ATN addresses or address prefixes in the ACA compressed format (7.8.3) with their expanded equivalent as defined below. Address markers and padding octets shall be

removed from the data stream during ACA decompression processing. The overall logic flow of the ACA decompression processing shall be as defined in 7.8.5.2. .

7.8.6.1. Address Decoding Process

The process of decoding a compressed ATN address or address prefix from the ACA compressed format (7.8.3) shall be performed using the sequence of steps defined in the following paragraphs. The steps shall be performed in the order listed below. The expanded address or prefix shall include the decoded address length octet and the decoded 7-20 address octets.

7.8.6.1.1. Decoding Address Length

If the FP subfield in the first header octet is zero, the octet length of the compressed address shall be set to 20 (a full ATN address). Otherwise, the octet length of the compressed address prefix shall be decoded from the LEN/SEL subfield in the first header octet according to the table in 7.8.3.1.1.3. The address octet length shall be used in the further decoding process steps.

If the IDRP subfield in the first header octet is zero, the output address length shall be the address octet length. Otherwise, the output address length shall be 8 times the address octet length.

Note.— The address octet length is an internal variable used in the decoding process. The output length prefixed to the expanded address after the decoding process is completed is either the same as the octet length (normal case) or 8 times the octet length (IDRP case, length in bits).

7.8.6.1.2. Decoding the AFI and IDI Fields

The AFI field of the decoded address shall be set to its constant value of [47] hexadecimal. The IDI field of the decoded address shall be set to its constant value of [0027] hexadecimal.

7.8.6.1.3. Decoding the VER Fields

If the CVER subfield in the first header octet is zero, the VER octet shall be extracted from the next octet in the variable field of the compressed address. If the CVER subfield is non-zero, then the VER field value in the expanded address shall be computed as follows:

a) If the T/I subfield in the second header octet is zero and the F/M subfield in the second header octet is zero, then the VER field value shall be set to the CVER value.

b) If the T/I subfield in the second header octet is zero and the F/M subfield in the second header octet is one, then the VER field value shall be set to the CVER value plus 64.

c) If the T/I subfield in the second header octet is one and the F/M subfield in the second header octet is zero, then the VER field value shall be set to the CVER value plus 128.

d) If the T/I subfield in the second header octet is one and the F/M subfield in the second header octet is one, then the VER field value shall be set to the CVER value plus 192.

7.8.6.1.4. Decoding the ADM Fields

If the ADMF subfield in the second header octet is set to zero, the three octets of the ADM field shall be extracted from the next three octets in the variable field data. Otherwise, the ADM field value shall be decoded from the compressed ADM which is extracted from the next two octets in the variable field data of the compressed address. The decoding of the compressed ADM value shall be performed as defined in 4.4.7. .

7.8.6.1.5. Decoding the RDF Fields

The RDF field in the expanded address shall be set to zero.

7.8.6.1.6. Decoding the ARS Fields

If the address length indicates an address prefix whose length is less than or equal to 8, no ARS field value shall be decoded and the decoding process shall halt.

If the ARSD subfield in the second header octet of the compressed address is set to one, the expanded ARS field shall be set to the default value ([000001] hexadecimal). Otherwise, the expanded ARS field value shall be extracted from the next three octets in the variable field data of the compressed address.

7.8.6.1.7. Decoding the LOC Fields

If the address length indicates an address prefix whose length is less than or equal to 11, no LOC field value shall be decoded and the decoding process shall halt.

If the LOCD subfield in the second header octet of the compressed address is set to one, the expanded LOC field shall be set to the default value ([0001] hexadecimal). Otherwise, the expanded LOC field value shall be extracted from the next two octets in the variable field data of the compressed address.

7.8.6.1.8. Decoding the SYS Fields

If the address length indicates an address prefix whose length is less than or equal to 13, no SYS field value shall be decoded and the decoding process shall halt.

If the SYS6 subfield in the second header octet has the value one, the high-order (6th) octet of the expanded SYS field shall be extracted from the

next octet in the variable data field of the compressed address. Otherwise, the high-order (6th) octet of the expanded SYS field shall be set to zero.

If the SYS5 subfield in the second header octet has the value one, the second to high-order (5th) octet of the expanded SYS field shall be extracted from the next octet in the variable data field of the compressed address. Otherwise, the second to high-order (5th) octet of the expanded SYS field shall be set to zero.

If the SYS4 subfield in the second header octet has the value one, the third to high-order (4th) octet of the expanded SYS field shall be extracted from the next octet in the variable data field of the compressed address. Otherwise, the third to high-order (4th) octet of the expanded SYS field shall be set to zero.

The remaining three octets of the expanded SYS field shall be extracted from the next three octets in the variable data field of the compressed address.

7.8.6.1.9. Decoding the SEL Fields

If the address length indicates an address prefix whose length is less than or equal to 19, no SEL field value shall be decoded and the decoding process shall halt.

If the FP subfield in the first header octet has the value zero (indicating a full ATN address), then the value of the SEL field shall be decoded from the LEN/SEL subfield in the first header octet. If the value of the LEN/SEL subfield lies in the range 1-2 the SEL value shall be decoded using the SEL encoding table in 7.8.3.1.1.3. If the LEN/SEL subfield encoding has the value 7, the SEL field value shall be extracted from the next octet in the variable data field of the compressed address.

Note.— Only a full ATN address (not a prefix) includes a SEL field.

7.8.6.2. Decompression Logic Flow

The ACA decompression logic shall process octets sequentially from the compressed data input stream. If the octet at the current input position and the next octet do not form a compressed address marker (7.8.4), the current input octet shall be copied to the decompressed output octet stream and decompression processing shall continue with the next input octet.

When a compressed address marker is found in the input octet stream, the decompression processing shall examine the value of the next octet beyond the address marker. If the value of this octet is zero (indicating an embedded address mark (7.8.4.2), the compressed address marker octets shall be copied to the decompressed output octet stream and the zero-value octet shall be dropped from the output stream. If the value is nonzero (indicating a compressed ATN address), the compressed address shall be decoded according to 7.8.6.1. The decoded address octets shall be copied to the decompressed octet output stream and decompression processing shall continue with the next input octet beyond those that formed the compressed ATN address. The compressed address marker octets shall not be copied to the output.

7.9. ATN SNDCF Protocol Requirements List - introduction

The Requirements for the ATN SNDCF are provided in the form of an ATN Profile Requirements List (APRLs). Three types of tables have been created :

- A first set of APRLs tables has been defined for mobile subnetworks, to summarize the requirements defined in the present Chapter of the CNS/ATM-1 Package SARPs and to indicate the strength of the requirements (mandatory, optional, conditional). The syntax used to describe these APRLs is the same as the one used by ISO for the ISO protocols PICS description.
- A second set of APRLs tables has been defined to summarize the SNDCF requirements relating to Subnetwork Routing Initiation and Termination .

7.10. ATN Requirements for mobile SNDCFs

This section specifies the requirements for the mobile SNDCF for the relevant CNS/ATM-1 Package IS's.

7.10.1. Major Capabilities

Item	**Capability**	**CNS/ATM-1 SARPs Ref.**	**CNS/ATM-1 Package Support**
*mcNego	Negotiation of Compression Algorithm	7.5.4.3.2	M
*mcLocRef	Local Reference Header Compression	7.5.4.~~.1~~	M
*mcCan	Local Reference Cancellation	7.5.4.5.4	O
*mcACA	ICAO Address Compression Algorithm	7.5.4.~~.1~~	O
mcV42	V.42bis Compression	7.5.4.~~.1~~	O

7.10.2. Call Setup and Clearing Procedures

Item	**Function**	**CNS/ATM-1 SARPs Ref.**	**CNS/ATM 1 Package Support**
csDynam	Dynamic Call Setup	7.5.4.3.2	M
csSys	Call Setup by Systems Management	7.5.4.3.2	O
csDef	Use of non-standard Default packet size	7.5.4.3.2	M
csFast	Use of Fast Select[1]	7.5.4.3.2	M
csOther	Use of other optional User Facilities and CCITT-specified DTE facilities	7.5.4.3.2	O
csCol	Call Collision Resolution	7.5.4.3.2	M

continued..

[1] Only required if supported by subnetwork

Call Setup and Clearing Procedures continued..

Item	Function	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
csAcp	Call Acceptance Procedures	7.5.4.3.5	M
csRej	Call rejection Procedures	7.5.4.3.6	M
csOrd	Order of compression Procedures	7.5.4.3.4	M
csDiag	Use of call rejection diagnostic codes	7.5.4.3.6	M
csReset	Call Reset Procedures	7.5.4.11	M

7.10.3. Negotiation of Compression Algorithm

Item	Function	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
caMaxd	Indication of the maximum of directories entries in the call user Data	7.5.4.3.3.1	mcNego:O

7.10.4. Local Reference Header Compression

Item	Function	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
lrVC	Opening additional virtual circuits	7.5.4.5	M
*lrDirSize	Local Directory with more than 128 entries	7.5.4.4	O
lrProt	Identification of Network Layer Protocol	7.5.4.5.1	M
lrMod	Processing of SN-UnitData Requests	7.5.4.5.2	M
lrEst	Establishment of new local reference	7.5.4.5.3	M
lrTransfer	Transfer of modified ISO 8473 PDU	7.5.4.5.5	M
lrInitial	Initial DT PDU Compression	7.5.4.6.1	M
lrDerived	Derived DT PDU Compression	7.5.4.6.2	M
*lrError-s	Generation of Error PDU Compression	7.5.4.6.2	M
lrDiscard	Compression of discarded PDU encapsulated within Error PDU	7.5.4.6.3	lrError-s:M
lrCompTr	Transfer of compressed PDUs	7.5.4.6.3.10	M
lrReceived	Processing of received PDUs	7.5.4.7	M
lrUncomp-r	Processing of received uncompressed PDUs	7.5.4.7.2	M
LrReset	Purging directories entries on Reset	7.5.4.11	mcMocRef:M

continued..

Local Reference Header Compression continued..

Item	Function	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
lrUnMod-r	Processing of received unmodified PDUs	7.5.4.7.2.1	M
lrComp-r	Processing of received compressed data PDUs	7.5.4.7.3	M
lrError-r	Processing of received compressed Error PDUs	7.5.4.7.4	M
lrSNDCFerr-s	Generation of SNDCF Error Report	7.5.4.8	M
lrSNDCFerr-r	Processing of received SNDCF Error Report	7.5.4.7.5	M

7.10.5. Local Reference Cancellation

Item	Function	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
lrcMgmt	Management of local references	7.5.4.5.4	mcCan:M
lrcRequest-s	Generation of Cancellation Request PDU	7.5.4.9	mcCan:M
lrcRequest-r	Processing of incoming Cancellation Request PDU	7.5.4.9	mcCan:M
lrcReliable	Reliable transfer of Cancellation Request	7.5.4.9	mcCan:M
lrcAccept-s	Generation of Cancellation Accept PDU	7.5.4.9	mcCan:M
lrcAccept-r	Processing of incoming Cancellation Accept PDU	7.5.4.9	mcCan:M

7.10.6. ICAO Address Compression Algorithm

Item	Function	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
acOut	Compression of outgoing PDUs	7.8.1	mcACA:M
acIn	Decompression of incoming PDUs	7.8.1	mcACA:M
acAddr	Address Length Determination	7.8.2	mcACA:M
acComp	Compression of NSAP Addresses and address prefixes	7.8.5	mcACA:M
acDecomp	Decompression of NSAP Addresses and address prefixes	7.8.6	mcACA:M

7.10.7. PDU Formats

7.10.7.1. Call Request User Data

Item	Description	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
crLen	Length Indicator	7.5.4.3.3	M
crVersion	Version Indicator	7.5.4.3.3	M
crSNCR	Subnetwork Connection Reference (SNCR)	7.5.4.3.3	M
crComp	Offerred Compression Techniques	7.5.4.3.3	M
crDir	Maximum Directory Size	7.5.4.3.3	M[2]
crAdd-s	Additional User Data on send	7.5.4.3.3	O
crAdd-r	Additional User Data on receive	7.5.4.3.3	O
MaxDir	Maximum number of directory entries supported	7.5.4.3.3	≥128

7.10.7.2. Call Accept User Data

Item	Description	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
caComp	Offerred Compression Techniques	7.5.4.3.3	mcNego:M
caAdd-s	Additional User Data on send	7.5.4.3.3	mcNego:O
caAdd-r	Additional User Data on receive	7.5.4.3.3	mcNego:O

7.10.7.3. Modified ISO 8473 NPDU

Item	Description	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
npLocRef-s	Local Reference Option field	7.5.4.5.2	M

[2] Dynamically, this field is only generated if Local Reference Compression is offered.

7.10.7.4. Compressed Initial PDU

Item	Description	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
inType	PDU Type	7.5.4.6.1.1	M
inPri	Priority	7.5.4.6.1.2	M
inLifetime	Lifetime	7.5.4.6.1.3	M
inFlags	Flag Bits	7.5.4.6.1.4 to 7.5.4.6.1.8	M
inLocRef	Local Reference (1 octet)	7.5.4.6.1.8	M
inLocRef2	Local Reference (2 octet)	7.5.4.6.1.8	lrDirSize:M ^lrDirsize:X
inPDUId	PDU Identifier	7.5.4.6.1.9	M
inNSDU	User Data	Figure 7.3	M

7.10.7.5. Compressed Derived PDU

Item	Description	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
drType	PDU Type	7.5.4.6.2.1	M
drPri	Priority	7.5.4.6.2.2	M
drLifetime	Lifetime	7.5.4.6.2.3	M
drFlags	Flag Bits	7.5.4.6.2.4 to 7.5.4.6.2.7	M
drLocRef	Local Reference (1 octet)	7.5.4.6.1.7	M
drLocRef2	Local Reference (2 octet)	7.5.4.6.1.7	lrDirSize:M ^lrDirsize:X
drPDUId	PDU Identifier	7.5.4.6.2.8	M
drSegOff	Segment Offset	7.5.4.6.2.9	M
drTotalLen	Total Length	7.5.4.6.2.10	M
drNSDU	User Data	Figure 7.3	M

7.10.7.6. Compressed Error PDU

Item	Description	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
erType	PDU Type	7.5.4.6.3.1	M
erPri	Priority	7.5.4.6.3.2	M
erLifetime	Lifetime	7.5.4.6.3.3	M
erFlags	Flag Bits	7.5.4.6.3.4 to 7.5.4.6.3.7	M
erLocRef	Local Reference (1 octet)	7.5.4.6.1.7	M
erLocRef2	Local Reference (2 octet)	7.5.4.6.1.7	lrDirSize:M ^lrDirsize:X
erReason	Discard Reason	7.5.4.6.3.8	M
erNSDU	Compressed Header of discarded PDU	7.5.4.6.3	M

7.10.7.7. SNDCF Error Report PDU

Item	Description	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
sfType	PDU Type	7.5.4.8	M
sfReason	Discard Reason	7.5.4.8	M
sfLocRef	Local Reference	7.5.4.8	M
sfLocRef2	Local Reference (2 octet)	7.5.4.6.1.8	lrDirSize:M ^lrDirsize:X

7.10.7.8. Cancellation Request

Item	Description	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
cqType	PDU Type	7.5.4.9	mcCan:M
cqRef	Cancellation Reference	7.5.4.9	mcCan:M
cqLocRef	Local Reference	7.5.4.9	M
cqLocRef2	Local Reference (2 octet)	7.5.4.6.1.8	lrDirSize:M ^lrDirsize:X

7.10.7.9. Cancellation Accept

Item	Description	CNS/ATM-1 SARPs Ref.	CNS/ATM-1 Package Support
ccType	PDU Type	7.5.4.9	mcCan:M
ccRef	Cancellation Reference	7.5.4.9	mcCan:M

8. ROUTING INFORMATION EXCHANGE PROTOCOL SPECIFICATION

8.1. Introduction

8.1.1. Scope

This chapter provides requirements and recommendations pertaining to the use of the ISO 10747 Inter-Domain Routing Protocol over Air-Ground and Ground-Ground Data Links, and the use of ISO 9542 in support of Route Initiation over Air-Ground Data Links. This chapter is concerned with the interoperability of protocol implementations and provides a compliance statement and APRL for each of the above protocols. It does not specify how Routing Information exchanged using ISO 10747 is used by Routers when forwarding ISO 8473 NPDUs, or the application of Routing Policy controlling Route Aggregation and re-advertisement of routes. These subjects are covered in Chapter 3.

8.1.2. Applicability of Requirements

All ATN Airborne Routers, with the exception of Airborne Routers implementing the procedures for non-use of IDRP, shall comply with the provisions contained in 8.2, 8.3, 8.3.1.2 to 8.3.1.5 inclusive, 8.3.1.8 to 8.3.1.11 inclusive, 8.3.2.1.1, 8.3.2.2 and the APRLs specified for an Airborne Router in 8.3.3. Airborne Routers implementing the procedures for non-use of IDRP shall be compliant with 8.2.

All ATN Air/Ground Routers shall comply with the provisions contained in 8.2, 8.3, 8.3.1.2 to 8.3.1.11 inclusive, 8.3.2.1.2, 8.3.2.2 and the APRLs specified for an Air/Ground Router in 8.3.3.

All Ground-Ground Inter-Domain Routers shall comply with the provisions contained in 8.2, 8.3.1.2 to 8.3.1.11 inclusive, 8.3.2.1.2, 8.3.2.2 and the APRLs specified for an Ground-Ground Router in 8.3.3.

8.2. End System to Intermediate System Routing Information Exchange Protocol (ES-IS)

8.2.1. ISO 9542 over mobile air-to-ground subnetworks

Airborne and Air/Ground ATN Routers directly connected to a mobile subnetwork (Mode S, AMSS or VDL) shall operate ISO 9542 over each such mobile subnetwork.

Configuration Information shall be exchanged by both Air/Ground and Airborne ATN Routers over each mobile subnetwork connection supporting an adjacency between them.

Note.— The use of ISO 9542 Configuration Information over mobile subnetworks in support of air/ground route initiation is specified in Chapter 3.

Route Redirection information shall not be exchanged between an Air/Ground and an Airborne Router.

8.2.2. ATN Protocol Requirements List - ISO 9542

In ATN Airborne and Air/Ground Routers, the ISO 9542 protocol implementation shall conform to the APRL given in Table 8-1 .

Note.— The requirements for ISO 9542 are provided in the form of a Protocol Requirements List.

Table 8-1: ISO 9542 - Intermediate System

Item	Protocol Function	Clauses	ISO Status	CNS/ATM-1 Package Support
CI	Is configuration information supported over the associated subnetwork?	CNS/ATM-1 SARPs Ref.: 8.2.1	O	M
RI	Is redirection information supported over the associated subnetwork?	CNS/ATM-1 SARPs Ref.: 8.2.1	O	OX
	Are the following functions supported?			
ErrP	Protocol Error Processing	6.13	M	M
HCsV	PDU Header Checksum Validation	6.12	M	M
HCsG	PDU Header Checksum Generation	6.12	O	O
RpCf	Report Configuration	6.2,6.2.2	CI:M	M
RcCf	Record Configuration	6.3,6.3.1	CI:M	M
FlCf	Flush Old Configuration	6.4	CI:M	M
RqRd	Request Redirect	6.8	RI:M	OX
CfNt	Configuration Notification	6.7	CI:O	OX
CTGn	ESCT Generation	6.3.2	CI:O	O
AMGn	Address Mask (only) generation	6.8	RI:O	OX
SMGn	Address mask and SNPA Mask generation	6.8	RI:O	OX
	Are the following PDUs Supported?			
ESH-r	<r> End System Hello	7.1,7.5	CI:M	O
ISH-<r>	<r> Intermediate System Hello	7.1,7.6	CI:O	M
ISH-<s>	<s> Intermediate System Hello	7.1,7.6	CI:M	M
RD-s	<s> Redirect	7.1,7.7	RI:M	OX
RD-r	<r> (ignore) Redirect	6.9,7.1,7.7	M	M

	Are the following PDU fields supported?			
FxPt	<s> Fixed Part <r> Fixed Part	7.2.1-7.2.7 7.2.1-7.2.7	M M	M M
SA-r	<r> Source Address, one or more NSAPs	7.3.1/2/3	CI:M	M
NET-s	<s> Network Entity Title	7.3.1/2/4	M	M
NET-r	<r> Network Entity Title	7.3.1/2/4	ISH-r:M	ISH-r:M
DA-s	<s> Destination Address	7.3.1/2/5	RI:M	OX
BSNPA-s	<s> Subnetwork Address	7.3.1/2/6	RI:M	OX
Scty-s	<s> Security	7.4.2	O	O
Scty-r	<r> Security	7.4.2	O	O
Pty-s	<s> Priority	7.4.3	O	O
Pty-r	<r> Priority	7.4.3	O	O
QoSM-s	<s> QOS Maintenance	7.4.4	RI:O	OX
AdMk-s	<s> Address Mask	7.4.5	RI:O	OX
SNMk-s	<s> SNPA Mask	7.4.6	RI:O	OX
ESCT-s	<s> Suggested ES Configuration Timer	7.4.7	CI:O	O
ESCT-r	<r> (ignore) Suggested ES Configuration Timer	7.4.7	ISH-r:M	ISH-r:M
OOpt-r	<r> (ignore) unsupported or unknown options	7.4.1	M	M
OOpt-s	<s> Other options		P	P
	Parameter Ranges			
HTv	What range of values can be set for the Holding Time Field in transmitted PDUs ?		M	M
CTv	If configuration information is supported, what range of values can be set for the Configuration Timer ?		CI:M	M

8.3. Intermediate-System to Intermediate-System Inter-Domain Routing Information Exchange Protocol

With the exception of Airborne Routers that implement the optional procedures for the non-use of IDRP, ATN Routers shall implement ISO/IEC 10747, including the ATN Specific Features specified in this section, and the APRLs specified in 8.3.3.

8.3.1. ATN Specific Features

8.3.1.1. Purpose of ATN Specific Features

ATN Airborne, Air-Ground and Ground-Ground Inter-Domain Routers shall implement the ATN Specific Features specified in the following subsections in order to support user requirements concerned with:

a) Ensuring that application data passed over air-ground data links conforms with any national and/or ITU restrictions applicable to that air-ground data link;

b) Ensuring that a classification scheme can be applied to routes throughout the ATN Ground Environment, reflecting the expected QoS available over each such route;

c) Ensuring that information on air-ground subnetwork types that a route passes over is available for determining which route to choose for a given application's data;

d) Ensuring that changes to routing information distributed for the above changes that report negative changes (e.g. a downgrading of the classification of a route) are reported in a timely manner.

8.3.1.2. Use of the Security Path Attribute

ATN Routers supporting inter-domain routing shall support the IDRP Security Path Attribute with a Security Registration Identifier set to the value defined in 6.2.2.5 for the ATN Security Registration Identifier. The Security Information provided with a so identified IDRP Security Path Attribute shall consist of zero one or more Security Tag Sets as defined in 6.2.2.5. The following Security Tag Sets shall be supported:

a) The Air-Ground Subnetwork type, as defined in 8.3.1.3.1.

b) The ATC Class, as defined in 8.3.1.3.2.

Recommendation. — *When an ATN Router supports data classified according to security policy and for the purpose of implementing mandatory access controls, then the ATN Router should also support the security classification security tag set defined in 6.2.2.5.*

When a route is available over more than one air-ground subnetwork type, then a separate Security Tag set shall be encoded into this field to identify each air-ground subnetwork that may support the route. When an air-ground subnetwork is restricted to carrying data of only certain traffic types, then the Security Tag set that identifies that air-ground subnetwork shall enumerate the Traffic Types that may pass over that subnetwork.

At most one ATC Class Security Tag Set shall be present in a route's Security Path Attribute.

An ATSC Class Security Tag Set shall not be present when one or more Air/Ground Subnetwork Security Tag Sets are also present, and when none of these Air/Ground Subnetwork Security Tag Sets indicates support of ATN Operational Communications - Air Traffic Service Communications.

8.3.1.3. Encoding of the Security Path Attribute Security Information Field

The Security Path Attribute Security Information Field shall comprise zero, one or more Security Tag Sets as defined in 6.2.2.5.

Note.— The Security Tag set format defined for use with CLNP in Chapter 6, has been adopted here as a convenient method for the extensible encoding of security related information.

8.3.1.3.1. Encoding of the Air/Ground Subnetwork Type

The Tag Set Name shall be set to [0000 0101], and the Security Tag is always two octets in length.

The first (lowest numbered) octet of the Security Tag shall indicate an air-ground subnetwork over which the route may be available according to Table 8-2.

Subnetwork Type	Security Tag (1st Octet)
Mode S	0000 0001
VDL	0000 0010
AMSS	0000 0011
Gatelink	0000 0100
HF	0000 0101

Table 8-2 Subnetwork Type Security Tag Values

The second (highest numbered) octet of the Security Tag shall indicate the Traffic Types allowed to pass over the air-ground subnetwork identified in the first octet. This octet shall comprise a bit map, where each bit corresponds to a different traffic type. A value of FFh shall be used to imply no restrictions. The assignment of bits to traffic type shall be according to Table 8-3, where bit 0 is the low order bit:

Bit Number	Traffic Type
0	ATN Operational Communications - Air Traffic Service Communications
1	ATN Operational Communications - Aeronautical Operational Control
2	ATN Administrative Communications
3	General Communications
4	ATN Systems Management

Table 8-3 Identification of Permissible Traffic Types

The semantics of bits 5 to 7 are reserved for future use and shall always be set to one.

8.3.1.3.2. Encoding of the ATSC Class Security Tag Set

The Tag Set Name shall be set to [0000 0110] and the Security Tag is always one octet in length. If a Security Tag with this Tag Set Name is received which is longer than one octet, then all octets after the first octet shall be ignored.

When this security tag set is present, the Security tag shall identify the ATSC classes supported by ~~of~~ the route. The ATSC Classes supported shall be identified according to table 8-4, where bit 0 is the low order bit, and setting a bit to one indicates that the corresponding ATSC Class is supported. A bit set to zero indicates that the corresponding ATSC Class is not supported.~~, as a single letter 'A' through to 'H' (upper case only) encoded according to International Alphabet No. 5 (IA5), and corresponding to the route's ATSC class. The octet shall be encoded with the high order bit set to zero and with the remaining low order seven bits set to the IA5 encoding of the character. For example, a route of ATSC Class A includes an ATSC Class Security Tag set in its Security Path Attribute's Security Information, with the value of the security tag being the IA5 encoded representation of the letter 'A'.~~

Bit Number	ATSC Class
0	A
1	B
2	C
3	D
4	E
5	F
6	G
7	H

Table 8-4 Identification of Supported ATSC Classes

8.3.1.4. Update of Security Information

8.3.1.4.1. The Air/Ground Subnetwork Type

When a Route is:

a) either advertised or received by an Air/Ground router over an adjacency supported by one or more air-ground subnetworks, and

b) contains a Security Path Attribute, and

c) has the ATN Security Policy Identifier, as the Security Path Attribute's Security Registration Identifier then,

The Security Path Attribute's Security Information shall be updated as follows:

1) An air-ground subnetwork Security Tag shall be added for each air-ground subnetwork supporting the adjacency and which is not already contained in the Security Information.

2) For each air-ground subnetwork Security Tag present in or added to the route, if ITU requirements or local policies restrict the Traffic Types that may pass over that subnetwork then the second octet of the security tag shall be modified to set to zero the bits corresponding to each traffic type not supported by that air-ground subnetwork.

8.3.1.4.2. The ATSC Class

When a route is advertised to an adjacent BIS, and according to local policy rules specified by a System Administrator and dependent on the BIS to which the route is being advertised and the route's NLRI, then:

a) if the route has been originated locally (i.e. within the same Routing Domain), or if the route has been originated by an ATN A/G BIS according to the procedures for the optional non-use of IDRP over an air-ground data link specified in section 3.5.2.11, an ATSC Class

security tag shall~~may~~ be added to the route identifying the ATSC Class specified by the System Administrator and formulated as part of the local policy rule.

b) if an ATSC Class security tag is present in the route, the class may be downgraded to a lower class, where Class A is the highest and Class H is the lowest.

c) if a route will be advertised over an adjacency supporting one or more Air/Ground subnetworks, and none of the Air/Ground subnetworks support ATSC traffic, then an ATSC Security Tag, if present in the route's security path attribute, shall be removed.

Downgrading shall be performed only when the route supports an ATSC Class higher than the highest ATSC Class supported by the local policy. When the ATSC Class is downgraded, the ATSC Security Tag Set shall be modified such that all bits indicating support for an ATSC Class higher than that supported by the local policy shall be set to zero, and the bit corresponding to the highest ATSC Class supported by local policy shall be set to one. All remaining bits shall be unaffected.

8.3.1.4.3. The Security Classification

When it is required by the local Security Policy that the router supports classified data, and a route is advertised to an adjacent BIS, and the highest level of protection offered by the subnetworks supporting the adjacency is lower than that reported by a Security Classification Security Tag, then that Security Tag shall be replaced by a Security Classification Security Tag reporting the highest protection offered by those subnetworks, as specified in the applicable security policy.

8.3.1.5. Route Selection

Note 1.— ISO/IEC 10747 clause 7.16.2 permits a loc-RIB that is identified by a RIB_ATT containing the Security Path Attribute, to contain more than one route to the same NLRI, provided that those routes provide the same level of protection.

When the Security Registration Identifier in an IDRP Security Path Attribute is the ATN Security Registration Identifier, and when no security classification is present in the route's security information, then all routes shall be assumed to offer the same level of protection.

Note 2.— the purpose of this statement is to permit, within the limitations imposed by IDRP, the existence in the loc-RIB of multiple routes to the same aircraft which differ ~~only~~ in the security related information.

During the Phase 2 Routing Decision process, when two or more routes to the same or overlapping destinations ~~of equal and the highest local preference,~~ are found in the adj-RIB-ins identified by a RIB_Att that includes the Security Path Attribute, but which differ in the security information contained in their security path attribute, then all such routes shall be selected and copied to the corresponding loc_RIB unless their computed preference is less than another such route which is usable by the same or more NPDUs.

Class	Name	Route Merging	Policy Based Route Aggregation	Policy Based Route Information Reduction
1.	Static Router			
2.	Level 1 Router			
3.	Level 2 Router			
4.	Ground-Ground Router	M	O	O
5.	Air/Ground-Router (ground based)	M	O	O
6.	Airborne Router with IDRP	M		
7.	Airborne Router without IDRP	M		

Table 8-5 ATN Routers and Route Aggregation

8.3.1.6. Route Aggregation and Route Information Reduction

ATN Routers shall implement the procedures for Route Aggregation and Route Information Reduction when required to do so according to Table 8-5.

Note 1.— Route Aggregation is defined by ISO 10747 as a procedure for the merging or aggregation of two routes in order to form a single replacement route. Route Aggregation may be applied as the result of a Routing Policy decision in order to reduce the routing information advertised to an adjacent Router. It is also necessary to aggregate two routes in the same loc_RIB and with identical NLRI prior to their being advertised to an adjacent Router. This latter case of Route Aggregation is automatic, not subject to Routing Policy, and necessary for the proper dissemination of routing information.

Note 2.— Route Information Reduction is defined by ISO 10747 as a procedure for replacing two or more NSAP Address Prefixes in a Route's NLRI by a single shorter NSAP Address Prefix. The decision on when to apply Route Information Reduction is also subject to Routing Policy and is typically associated with the application of Route Aggregation when applied as a result of Routing Policy.

8.3.1.6.1. Policy Based Route Aggregation

Recommendation.— *An Air/Ground Router should aggregate all routes to destinations in Routing Domains in its own ATN Island, other than those to destinations in its own Routing Domain., ~~and similarly perform route information reduction as permitted by the ATN Addressing Plan, before advertising such routes to an airborne Routing Domain.~~*

~~Note 1.— It is intended that the result of Route Information Reduction is a single NSAP Address Prefix to all destinations on the ATN Island. However, this will only be possible if NSAP Addresses have been allocated within the ATN Island with a single common prefix for all such addresses.~~

Recommendation.— *An Air/Ground Router should aggregate all routes to destinations in ATN Islands, other than its own ATN Island~~, and similarly perform route information reduction as permitted by the ATN Addressing Plan, before advertising such routes to an airborne Routing Domain.~~*

~~Note 2.— It is intended that the result of Route Information Reduction is a single NSAP Address Prefix to all destinations within the ATN.~~

Recommendation.— *ATN Ground-Ground Routers should perform Route Aggregation and Route Information Reduction on routes to ground destinations, in line with local policy requirements*

for reducing the amount of routing information distributed within the ATN Ground Environment.

Note 1~~3~~.— The need for this will be determined according to local topology and NSAP Address Assignment and is outside of the scope of this specification. However, this feature is a necessary condition for the development of a large scale and scaleable internet.

The selection of candidate routes for aggregation shall be performed separately for each adjacent BIS according to a filter on each route's destination, with a combination of inclusion and exclusion filters.

Note 2. — For example. filters might be applied in order to select all routes to NSAP Address Prefixes within the local ATN Island, while excluding those to the local Administrative Domain.

8.3.1.6.2. Aggregation of Routes in the Same Loc-RIB with Identical NLRI

When two or more routes exist in the same loc_RIB and which have identical NLRI, then such routes shall be aggregated after~~before~~ the application of local policy rules that select routes for re-advertisement to each adjacent BIS, and their consequently being copied to the associated~~an~~ adj-RIB-out. For each Adjacent BIS, the resulting aggregated route shall be inserted into the associated Adj-RIB-out. In order to aggregate such routes, an ATN Router shall apply one of the following two strategies:

a) **True Route Aggregation:** the routes are aggregated according to ISO 10747 route aggregation procedures and the procedures for aggregation of the security path attribute specified in 8.3.1.6.3 below.

b) **Route Merging:** the routes are merged by arbitrarily selecting one of these routes and updating its security path attribute to the value that would have resulted had the routes been aggregated, as above. The selected route with its updated security path attribute is then the result of the merging procedure.

Note 1.— The former of the two strategies is preferred.

Note 2.— The second strategy has been introduced as an interim measure to simplify initial implementations. However, this second strategy leads to a situation where routing decisions based on RD_Path information cannot be performed, as this information is lost in the merging process. The second strategy may therefore be deleted in a later revision of these SARPs.

Note 3.— Whenever local policy rules that select routes for advertisement to adjacent BISs select different combinations of routes from the same loc_RIB and with identical NLRI, for advertisement to different adjacent BISs, then the Route Aggregation or Merging procedure has to be carried out separately for each Adj-RIB-out. For each Adj-RIB-out, only those routes which are eligible for advertisement to the corresponding BIS will be input to the merging/aggregation procedure. For example, a route may not be eligible for advertisement to an adjacent BIS due to distribution restrictions or a potential route loop recognised from the RD_PATH information.

Note 4.— An aggregated route resulting from these procedures may also be aggregated with other routes in an Adj-RIB-out, due to the application of local policy rules.

8.3.1.6.3. Aggregation of the Security Path Attribute Information Field

The aggregation rules for the security information field contained in security path attributes that include the ATN Security Registration identifier shall be:

a) The aggregated security path attribute shall comprise each air-ground subnetwork security tag contained in the security path attribute of the component routes.

b) When an air-ground subnetwork security tag for the same air-ground subnetwork occurs in both component routes, then these shall be combined by a logical "OR" of the second octet of the security tags. Only a single air-ground subnetwork security tag for each distinct air-ground subnetwork shall be present in the aggregated route.

c) When aggregating an ATSC Class Security Tag,

1) If the NLRI of the component routes is not identical then, when an ATSC Class security tag occurs in all component routes the aggregated route shall contain an ATSC Class security tag. The ATSC Class of the aggregated route shall be the lowest ATSC Class of the aggregated route's component routes, indicated by setting the value of the corresponding bit in the security tag value to one. All the other bits in this tag shall be set to zero. If an ATSC Class security tag is not present in any component route then the aggregated route shall not contain an ATSC Class security tag.

Note.— If routes with dissimilar NLRI are aggregated, then the aggregated route will not be available to applications requiring a higher ATSC Class than that provided by the

aggregated route, but which may have been available in the component routes.

2) Otherwise, when an ATSC Class security tag occurs in one or more component routes then the aggregated route shall contain an ATSC Class security tag. The ATSC Class of the aggregated route shall be formed by a logical 'OR' of the encoded representation of the supported ATSC Class in each of the aggregated route's component routes that contain an ATSC Class security.~~an ATSC Class security tag occurs in all component routes then the aggregated route shall contain an ATSC Class security tag. The ATSC Class of the aggregated route shall be the lowest ATSC Class of the aggregated route's component routes. If an ATSC Class security tag is not present in any component route then the aggregated route shall not contain an ATSC Class security tag.~~

d) When a Security Classification security tag occurs in all component routes then the aggregated route shall contain a Security Classification security tag. This shall be set to the lowest classification from the classifications given to the aggregated route's component routes. If a Security Classification security tag is not present in at least one~~any~~ component route then the aggregated route shall not contain a Security Classification security tag.

8.3.1.6.4. Route Information Reduction

Recommendation. — An Air/Ground Router should perform route information reduction as permitted by the ATN Addressing Plan, before advertising aggregated routes to an airborne Routing Domain.

Note 1.— It is intended that the result of Route Information Reduction is a single NSAP Address Prefix to each destination group to which aggregation is performed. However, this will only be possible if NSAP Addresses have been allocated appropriately (e.g. all systems within the same ATN Island with a single common prefix for all such addresses).

Route Information Reduction shall be performed using local policy rules, with such routing policy rules required to specify when a set of NSAP Address Prefixes is replaced by a shorter NSAP Address Prefix. Two types of rules shall be supported:

a) The explicit replacement of a set of NSAP Address Prefixes by another shorter NSAP Address Prefix, only when all members of the set are present;, or

b) The explicit replacement of a set of NSAP Address Prefixes by another shorter NSAP Address Prefix when any members of the set are present.

8.3.1.7. Frequency of Route Advertisement

*Note.— ISO/IEC 10747 clause 7.17.3.1 requires that the advertisement of feasible routes to some common set of destinations received from BISs in other Routing Domains must be separated in time by at least **minRouteAdvertisementInterval** except for certain identified cases. The list of exceptions to this requirement is extended by this specification.*

If a selected route to a given destination changes in respect of the Security Information contained in its Security Path Attribute, then that route shall be immediately re-advertised to all adjacent BISs to which that route had previously been advertised and not since withdrawn. The procedure for ensuring a minimum time interval of **minRouteAdvertisementInterval** between successive advertisements of routes to the same destination shall not apply in this case.

8.3.1.8. Interpretation of Route Capacity

For the ATN environment, the CAPACITY path attribute shall contain one of the values listed in Table 8-64, and shall assumed to have the semantics given there:

Value	Meaning
1-9	Unassigned
13	0 - 19.2 KBits/sec
12	19.2 - 56 Kbits/sec
11	56 - 1500 Kbits/sec
10	> 1500 Kbits/sec
14 .. 255	Unassigned

Table 8-64 Interpretation of Capacity Route Metric

Note.— The CAPACITY path attribute is a well known mandatory attribute that is used to denote the traffic handling capacity of the RD_PATH listed in the same UPDATE PDU. Higher values indicate a lower traffic handling capacity than do low values.

8.3.1.9. Network Layer Reachability Information (NLRI)

In support of ATN communications, ATN Routers shall encode the NLRI **Addr_info** field of each route as a list of NSAP Address Prefixes. The **proto_type**, and **proto_length** fields shall be set to 1 and the **Protocol** field shall be set to X'81' in order to signal support of ISO 8473.

8.3.1.9.1. NSAP Address Prefix Alignment

When originating a route or performing route information reduction, an ATN Router shall only generate NSAP address prefixes that are octet-aligned.

Note 1.— For IDRP, ATN NSAP prefixes will be eleven octets (or less).

Note 2.— 8.3.1.11specifies the RIB-Atts that an ATN Router must support.

Note 3.— The above requirement does not modify the requirement in ISO/IEC 10747 to be able to accept and correctly handle a non-octet aligned NSAP Address Prefix.

Note 4.— The above requirement simplifies prefix matching.

8.3.1.10. BISPDU Authentication

ATN Routers shall support the validation of BISPDUs using Authentication Type 1. When an ATN Router initiates a BIS-BIS connection, it shall set the value of the Authentication Code in the OPEN PDU to 1, in order to indicate that the Validation field in the header of all BISPDU sent over the BIS-BIS connection will contain an unencrypted checksum. .

When an authentication code of 1 is specified in the Authentication Code of the OPEN BISPDU that initiated a BIS-BIS connection then, an ATN Router shall generate a validation pattern according to clause 7.7.1 of ISO 10747, for each BISPDU that it sends over that connection, and similarly validate the validation pattern of all received BISPDUs on such a connection.

Note1.— Support of Authentication Codes 2 and 3 is outside of the scope of this specification and their use is a local matter.

The type 1 authentication code shall be generated according to the MD4 specification published in RFC 1320.

Note2.— The interpretation of MD4 given in Annex B of ISO 10747 is open to ambiguous interpretation and may lead to interoperability problems.

Note3. — RFC 1320 supersedes RFC 1186 which was the basis for ISO 10747 Annex B. Specifications of MD4 algorithm contained in these two RFC documents are technically equivalent.

8.3.1.11. Restrictions on Route Advertisement

A route shall not be advertised to a BIS in another RD where:

a) The route contains the receiving RD's RDI in its RD_PATH path attribute, or

b) The route's RD_PATH path attribute contains the RDI of a confederation which is being entered when the route is advertised to the other RD.

Note.— This is essential to avoid long lived black holes following the explicit withdrawal of an unfeasible route and when many alternate paths are available (e.g. within an ATN Island Backbone).

8.3.1.12. RIB_ATT Support

	ISO Mandatory Requirement	Notes
1.	Internal Update Procedures	*Note 1.— There is only ever a single Boundary Router on board an aircraft, and hence, internal update is not applicable.*
2.	Operation of **minRouteAdvertisementInterval** Timer	*Note 2.— An Aircraft is always an End Routing Domain, and hence will never re-advertise routes*
3.	Recognition of Next Hop Attribute	*Note 3.— No Requirement for Support in ATN*
4.	Recognition of Residual Error, Expense, Transit Delay and Priority Distinguishing Path Attributes	*Note 4.— Never negotiated for use in the ATN.*
5.	Support of RIB Refresh	*Note 5.— RIB Refresh is necessary for long lived adjacencies rather than the short lived adjacencies anticipated for ATN Mobiles.*
6.	Support of DIST_LIST_EXCL	*Note 6.— There are no known User Requirements to control the distribution of routes to or from Mobile Systems. Implementation may also be problematic due to changing point of attachment to ATN.*
7.	Support of Partial Source Routing	*Note 7.— There are no known user requirements for partial source routing.*

Table 8-75 ISO 10747 Mandatory Requirements, for Which ~~Excluded for~~ Support is Optional for~~by~~ ATN Airborne Routers

An ATN Router incorporating IDRP shall support the following RIB_Att sets~~, and shall attempt to negotiate the use of all those RIB_Atts it supports when opening a BIS-BIS connection~~:

a) The empty RIB-Att

b) SECURITY

and shall attempt to negotiate the use of all those RIB_Atts it supports when opening a BIS-BIS connection.

The semantics of the empty RIB_Att shall be taken as implying that routes advertised under the empty RIB_Att have a classification of "Unclassified", have not passed over any Mobile Subnetworks and have been classed as ATSC Class H.

8.3.1.13. Additional Update PDU Error Handling

When an Update PDU is received with a Security Path Attribute with an ATN Security Registration Identifier and Security Information that contains:

a) an ATSC Class Security Tag Set, and

b) One or more Air/Ground Subnetwork Security Tag Sets, such that none of these security tag sets indicates support of ATN Operational Communications - Air Traffic Service Communications, then the Update PDU shall be discarded and an IDRP ERROR PDU generated with an Error_Code indicating an UPDATE_PDU_Error, and an error subcode set to 64.

8.3.1.14. CLNP Data PDU Parameters

The CLNP Data PDU that carries a BISPDU between two ATN Routers shall include:

a) A Security Parameter providing an ATN Security Label indicating a traffic type of "Systems Management"

b) A priority parameter indicating a PDU priority of 14.

8.3.2. Compliance with ISO/IEC 10747

The IDRP protocol exchange shall use the connectionless network service provided by ISO 8473 as specified in ISO/IEC 10747.

8.3.2.1. ISO 10747 Mandatory Requirements

8.3.2.1.1. Airborne Router

An ATN Airborne Router supporting the ISO 10747 Inter-Domain Routing Protocol shall support all mandatory requirements as specified in clause 12.1 of ISO 10747 with the exception of the requirements listed in Table 8-75, for which support is optional.

Note 7.— This specification deviates from ISO 10747 for Airborne Routers, in order to simplify

the specification of operational equipment by removing all non-applicable requirements.

Note 8.— Representations are being made to ISO regarding possible over-specification in ISO 10747.

8.3.2.1.2. Ground Router

Note.— This section refers to both Air/Ground and Ground-Ground Routers generically as Ground Routers.

An ATN Ground Router supporting the ISO 10747 Inter-Domain Routing Protocol shall support all mandatory requirements as specified in clause 12.1 of ISO 10747. However, over adjacencies with Airborne Routers, ATN Air/Ground Routers are specifically excluded from dynamic use of the following functions and features:

a) The Next Hop Path Attribute

b) The DIST_LIST_EXCL Path Attribute

c) RIB Refresh Request

d) The Residual Error Path Attribute

e) The Expense Path Attribute

f) The Priority Path Attribute

g) The Transit Delay Path Attribute.

h) The Locally Defined QoS Path Attribute.

i) Hierarchical Recording

j) Support of Partial Source Routing

8.3.2.2. ISO 10747 Optional Requirements

An ATN Router shall support the Security Path Attribute as specified in 8.3.1.2 and 8.3.1.3.

Recommendation.— *An ATN Air/Ground Router should implement Route Aggregation and Route Information Reduction Procedures.*

Recommendation.— *An ATN Ground-Ground Router should implement Route Aggregation and Route Information Reduction Procedures.*

8.3.3. APRLs

Note.—The IDRP requirements list is a statement of which capabilities and options of the protocol at minimum are required to be implemented for the ATN environment. The requirements list may be used by the protocol implementor as a check list to conform to this standard; by the supplier and procurer to provide a detailed indication of the capabilities of an implementation; by the user to check the possibility of interworking between two different implementations; and by the protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance to the protocol.

8.3.3.1.1. ATN Specific Protocol Requirements

Index	Item	CNS/ATM-1 SARPs Ref	G-G Router	A/G Router	Airborne Router
ATNIDRP1	Encoding and use of the Security Path Attribute	8.3.1.2, 8.3.1.3	M	M	M
ATNIDRP2	Additional procedures for non-use of the **minRouteAdvertisementInterval** Timer	8.3.1.5	M	M	-
ATNIDRP3	Support of Route Aggregation and Route Information Reduction	8.3.2.2	O	O	-
ATNIDRP4	Support for Route Merging Procedures	8.3.1.6	M	M	-

8.3.3.1.2. IDRP General

Item	Description	ISO 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
BASIC	Are all basic BIS functions implemented?	12.1	M	M	M	M
MGT	Is this system capable of being managed[1] by the specified management information?	11	M	O	O	O
VER	Does this BIS support Version Negotiation?	7.8	M	M	M	M

1 The interpretation of this Item is that mandatory compliance requires that access to the MO is provided via a Systems Management Agent. Remote Systems Management is not required for CNS/ATM-1 Package and hence it is not reasonable to require mandatory support for this requirement.

Item	Description	ISO 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
RTSEP	Does this BIS support ROUTE_SEPARATOR attribute?	7.12.1	M	M	M	M
HOPS	Does this BIS support the RD_HOP_COUNT attribute?	7.12.13	M	M	M	M
PATH	Does this BIS support the RD_PATH attribute?	7.12.3	M	M	M	M
CAPY	Does this BIS support the Capacity Attribute?	7.12.15	M	M	M	M
FSM	Does this BIS manage BIS-BIS connections according to the BIS FSM description?	7.6.1	M	M	M	M
FCTL	Does this BIS provide flow control?	7.7.5	M	M	M	M
SEQNO	Does this BIS provide sequence number support?	7.7.4	M	M	M	M
INTG1	Does this BIS provide Data integrity using authentication type 1?	7.7.1	O.1	M	M	M
INTG2	Does this BIS provide Data integrity using authentication type 2?	7.7.2	O.1	O	O	O
INTG3	Does this BIS provide Data integrity using authentication type 3?	7.7.3	O.1	O	O	O
ERROR	Does this BIS handle error handling for IDRP?	7.20	M	M	M	M
RIBCHK	Does this BIS operate in a "fail-stop" manner with respect to corrupted routing information?	7.10.2	M	M	M	M

8.3.3.1.3. IDRP Update Send Process

	Item	ISO 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
INT	Does the BIS provide the internal update procedures?	7.17.1	M	M	M	O
RTSEL	Does this BIS support the **MinRouteAdvertisementInterval** Timer?	7.17.3.1	M	M	M	O
RTORG	Does this BIS support the **MinRDOriginationInterval** Timer?	7.17.3.2	M	M	M	M
JITTER	Does this BIS provide jitter on its timers?	7.17.3.3	M	M	M	M

8.3.3.1.4. IDRP Update Receive Process

Item	Description	ISO 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
INPDU	Does the BIS handle inbound BISPDUs correctly?	7.14	M	M	M	M
INCONS	Does this BIS detect inconsistent routing information?	7.15.1	M	M	M	M

8.3.3.1.5. IDRP Decision Process

Item	Description	ISO 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
TIES	Does this BIS break ties between candidate routes correctly?	7.16.2.1	M	M	M	M
RIBUPD	Does this BIS update the Loc-RIBs correctly?	7.16.2	M	M	M	M
AGGRT	Does this BIS support route aggregations?	7.18.2.1, 7.18.2.2, 7.18.2.3	O	ATNIDRP3: M	ATNIDRP3: M	-
LOCK	Does this BIS provide interlocks between its Decision Process and the updating of the information in its Adj-RIBs-In?	7.16.4	M	M	M	M

8.3.3.1.6. IDRP Receive

Item	Description	ISO 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
RCV	Does the BIS process incoming BISPDUs and respond correctly to error conditions?	7.14, 7.20	M	M	M	M
OSIZE	Does this BIS accept incoming OPEN PDUs whose size in octets is between **MinBISPDULength** and 3000?	6.2,7.20	M	M	M	M
MXPDU	Does the BIS accept incoming UPDATE, IDRP ERROR and RIB REFRESH PDUs whose size in octets is between **minBISPDULength** and **maxBISPDULength**?	6.2,7.20	M	M	M	BISREF: OX ^BISREF:M

BISREF: if RIB REFRESH PDU **then** true **else** false

8.3.3.1.7. Peer Entity Authentication

Item	Description	ISO 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
AUTH	Does this BIS correctly authenticate the source of a BISPDU?	7.7.2	O	M	M	M

Note.— Only support for an Authentication Code 1 is required.

8.3.3.1.8. IDRP CLNS Forwarding

Item	Description	ISO 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
PSRCRT	Does the BIS correctly handle 8473 NPDUs that contain a partial source route?	8	M	O	O	O
DATTS	Does the BIS correctly extract the NPDU-derived Distinguishing Attributes from an 8473 NPDU?	8.2	M	M	M	M
MATCH	Does the BIS correctly match the NPDU-derived Distinguishing Attributes with the corresponding FIB-Atts?	8.3	M	M	M	M
EXTF	Does the BIS correctly forward NPDUs with destinations outside its own routing domain?	8.4	M	M	M	M
INTF	Does the BIS correctly forward NPDUs with destinations inside its own routing domain?	8.1	M	M	M	M

8.3.3.1.9. IDRP Receive Process

Item	Description	ISO 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
RCV	Does the BIS process incoming BISPDUs and respond correctly to error conditions?	7.14, 7.20	M	M	M	M
OSIZE	Does this BIS accept incoming OPEN PDUs whose size in octets is between **MinBISPDULength** and 3000?	6.2,7.20	M	M	M	M
MXPDU	Does the BIS accept incoming UPDATE, IDRP ERROR and RIB REFRESH PDUs whose size in octets is between **minBISPDULength** and **maxBISPDULength**?	6.2,7.20	M	M	M	M

8.3.3.1.10. IDRP Optional Transitive Attributes

Item	Description	ISO 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
MEXIT	Does this BIS support use of the MULTI-EXIT DISC attribute?	7.12.7	O	O	O	O

8.3.3.1.11. Generating Well-Known Discretionary Attributes

Item	Description	ISO 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
EXTG	Does the BIS support generation of the EXT_INFO attribute?	7.12.2	O	O	O	O
NHRS	Does the BIS support generation of the NEXT_HOP attribute in support of route servers?	7.12.4	O	O	IDRPAG:OX ^IDRPAG:O	O
NHSN	Does the BIS support generation of the NEXT_HOP attribute to advertise SNPAs?	7.12.4	O	O	IDRPAG:OX ^IDRPAG:O	O
DLI	Does the BIS support generation of the DIST_LIST_INCL attribute?	7.12.5	O	O	O	O
DLE	Does the BIS support generation of the DIST_LIST_EXCL attribute?	7.12.6	O	O	IDRPAG:OX ^IDRPAG:O	O
TDLY	Does the BIS support generation of the TRANSIT DELAY attribute?	7.12.8	O	O	IDRPAG:OX ^IDRPAG:O	O
RERR	Does the BIS support generation of the RESIDUAL ERROR attribute?	7.12.9	O	O	IDRPAG:OX ^IDRPAG:O	O
EXP	Does the BIS support generation of the EXPENSE attribute?	7.12.10	O	O	IDRPAG:OX ^IDRPAG:O	O
LQOSG	Does the BIS support generation of the LOCALLY DEFINED QOS attribute?	7.12.11	O	OX	OX	OX
HREC	Does the BIS support generation of the HIERARCHICAL RECORDING attribute?	7.12.12	O	OX	OX	OX
SECG	Does the BIS support generation of the SECURITY attribute?	7.12.14	O	M	M	M
PRTY	Does the BIS support generation of the PRIORITY attribute?	7.12.16	O	O	IDRPAG:OX ^IDRPAG:O	O

IDRPAG: if Air/Ground adjacency **then** true **else** false

8.3.3.1.12. Propagating Well-Known Discretionary Attributes

Item	Description	ISO 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
EXTGP	Does the BIS support propagation of the EXT_INFO attribute?	7.12.2	M	M	M	-
NHRSP	Does the BIS support propagation of the NEXT_HOP attribute in support of route servers?	7.12.4	O	O	IDRPAG:OX ^IDRPAG:O	-
NHSNP	Does the BIS support propagation of the NEXT_HOP attribute to advertise SNPAs?	7.12.4	O	O	IDRPAG:OX ^IDRPAG:O	-
DLIP	Does the BIS support propagation of the DIST_LIST_INCL attribute?	7.12.5	O	M	M	-
DLEP	Does the BIS support propagation of the DIST_LIST_EXCL attribute?	7.12.6	O	M	IDRPAG:OX ^IDRPAG:M	-
TDLYP	Does the BIS support propagation of the TRANSIT DELAY attribute?	7.12.8	O	O	IDRPAG:OX ^IDRPAG:O	-
RERRP	Does the BIS support propagation of the RESIDUAL ERROR attribute?	7.12.9	O	O	IDRPAG:OX ^IDRPAG:O	-
EXPP	Does the BIS support propagation of the EXPENSE attribute?	7.12.10	O	O	IDRPAG:OX ^IDRPAG:O	-
LQOSP	Does the BIS support propagation of the LOCALLY DEFINED QOS attribute?	7.12.11	O	OX	OX	-
HRECP	Does the BIS support propagation of the HIERARCHICAL RECORDING attribute?	7.12.12	O	OX	OX	-
SECP	Does the BIS support propagation of the SECURITY attribute?	7.12.14	O	M	M	-
PRTYP	Does the BIS support propagation of the PRIORITY attribute?	7.12.16	O	O	IDRPAG:OX ^IDRPAG:O	-

8.3.3.1.13. Receiving Well-Known Discretionary Attributes

Item	Description	ISO 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
EXTR	Does the BIS recognise upon receipt the EXT_INFO attribute?	7.12.2	M	M	M	M
NHRSR	Does the BIS recognise upon receipt the NEXT_HOP attribute ?	7.12.4	M	M	M	O
DLIR	Does the BIS recognise upon receipt the DIST_LIST_INCL attribute?	7.12.5	M	M	M	M
DLER	Does the BIS recognise upon receipt the DIST_LIST_EXCL attribute?	7.12.6	M	M	M	O
TDLYR	Does the BIS recognise upon receipt the TRANSIT DELAY attribute?	7.12.8	M	M	M	O
RERRR	Does the BIS recognise upon receipt the RESIDUAL ERROR attribute?	7.12.9	M	M	M	O
EXPR	Does the BIS recognise upon receipt the EXPENSE attribute?	7.12.10	M	M	M	O
LQOSR	Does the BIS recognise upon receipt the LOCALLY DEFINED QOS attribute?	7.12.11	M	O	O	O
HRECR	Does the BIS recognise upon receipt the HIERARCHICAL RECORDING attribute?	7.12.12	M	M	M	O
SECR	Does the BIS recognise upon receipt the SECURITY attribute?	7.12.14	M	M	M	M
PRTYR	Does the BIS recognise upon receipt the PRIORITY attribute?	7.12.16	M	M	M	O

8.3.3.1.14. IDRP Timers

Item	Description	ISO 10747 Ref.	ISO Status	G-G Router	A/G Router	Airborne Router
Ta	KeepAlive time	7.6.5	M	M	M	M
Tr	Retransmission (tr) timer	7.6.5	M	M	M	M
Tmr	maxRIBIntegrityCheck timer	7.10.2	M	M	M	M
Tma	MinRouteAdvertisement timer	7.17.3.1	M	M	M	O
Trd	MinRDOriginationInterval timer	7.17.3.2	M	M	M	M
Tcw	closeWaitDelay timer	7.6.4	M	M	M	M

9. SYSTEMS MANAGEMENT PROVISIONS

9.1. Introduction

Recommendation.— *ATN managed resources should be grouped into management domains in order to assign responsibility for control of the resources. An organization should assign an administrative authority to establish and maintain the respective management authorities of each of its management domains, and to manage the transfer of control of resources from one management domain to another.*

Note.— Given the current lack of well identified operational requirements regarding Systems Management for the ATN internet , the definition and implementation of a global ATN Systems Management solution cannot be achieved within the timeframe foreseen for the CNS/ATM-1 Package SARPs. Consequently within this timeframe:

a) No exchange of Systems Management information will be required between routers of different administrative domains .

b) No exchange of Systems Management information will be required by means of a management protocol over the air-ground links. This does not preclude the exchange of routing information, by means of routing information exchange protocols.

c) The exchange of Systems Management information within an administrative domain is considered a local matter and can be achieved by any means deemed appropriate.

Note.— Nevertheless, it is desirable to implement provisions which enable the exchange of Systems Management information across administrative domain boundaries as long as it does not compromise the safety and regularity of flight.